CA IdentityMinder™

Administrationshandbuch

12.6.3

Diese Dokumentation, die eingebettete Hilfesysteme und elektronisch verteilte Materialien beinhaltet (im Folgenden als "Dokumentation" bezeichnet), dient ausschließlich zu Informationszwecken des Nutzers und kann von CA jederzeit geändert oder zurückgenommen werden. Diese Dokumentation ist Eigentum von CA und darf ohne vorherige schriftliche Genehmigung von CA weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden.

Der Benutzer, der über eine Lizenz für das bzw. die in dieser Dokumentation berücksichtigten Software-Produkt(e) verfügt, ist berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen innerbetrieblichen Gebrauch im Zusammenhang mit der betreffenden Software auszudrucken, vorausgesetzt, dass jedes Exemplar diesen Urheberrechtsvermerk und sonstige Hinweise von CA enthält.

Dieses Recht zum Drucken oder anderweitigen Anfertigen einer Kopie der Dokumentation beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenz. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Lizenznehmer gegenüber CA schriftlich, dass alle Kopien oder Teilkopien der Dokumentation an CA zurückgegeben oder vernichtet worden sind.

SOWEIT NACH ANWENDBAREM RECHT ERLAUBT, STELLT CA DIESE DOKUMENTATION IM VORLIEGENDEN ZUSTAND OHNE JEGLICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN INSBESONDERE STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET CA GEGENÜBER IHNEN ODER DRITTEN GEGENÜBER FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER NUTZUNG DIESER DOKUMENTATION ENTSTEHEN; DAZU GEHÖREN INSBESONDERE ENTGANGENE GEWINNE, VERLORENGEGANGENE INVESTITIONEN, BETRIEBSUNTERBRECHUNG, VERLUST VON GOODWILL ODER DATENVERLUST, SELBST WENN CA ÜBER DIE MÖGLICHKEIT DIESES VERLUSTES ODER SCHADENS INFORMIERT WURDE.

Die Verwendung aller in der Dokumentation aufgeführten Software-Produkte unterliegt den entsprechenden Lizenzvereinbarungen, und diese werden durch die Bedingungen dieser rechtlichen Hinweise in keiner Weise verändert.

Diese Dokumentation wurde von CA hergestellt.

Zur Verfügung gestellt mit „Restricted Rights“ (eingeschränkten Rechten) geliefert. Die Verwendung, Duplizierung oder Veröffentlichung durch die US-Regierung unterliegt den in FAR, Absätze 12.212, 52.227-14 und 52.227-19(c)(1) bis (2) und DFARS, Absatz 252.227-7014(b)(3) festgelegten Einschränkungen, soweit anwendbar, oder deren Nachfolgebestimmungen.

Copyright © 2013 CA. Alle Rechte vorbehalten. Alle Markenzeichen, Markennamen, Dienstleistungsmarken und Logos, auf die hier verwiesen wird, sind Eigentum der jeweiligen Unternehmen.

CA Technologies-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA Technologies:

- CA CloudMinder™ Identity Management
- CA Directory (NeteAuto-Verzeichnis)
- CA IdentityMinder ™
- CA GovernanceMinder (früher "CA Role & Compliance Manager")
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder ™

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Inhalt

Kapitel 1: Planen von Rollen 17

Entscheidungen in Bezug auf Rollen 17
Zweck der Rollen 18
Erstellen von zusätzlichen Administratoren 19
Rollen für Identitäts- oder Zugriffsmanagement 20
Delegierte Verwaltung 20
Festlegen eines Rollenadministrators 21
Delegierungsschritte 22
Delegierungsbeispiel 23
Rollenmerkmale 23
Rollenprofil 24
Aufgaben für die Rolle 24
Kontovorlagen 24
Mitglieder-, Admin- und Eigentümerregeln 25
Bereichsregeln 26
Allgemeine Richtlinien zu Regeln 30
Hinzufügungs- und Entfernungsaktionen 30
Mitgliederrichtlinien 31
Admin-Richtlinien 32
Checkliste für die Rollenplanung 33

Kapitel 2: Admin-Rollen 35

Admin-Rollen und Admin-Aufgaben 35
Admin-Rollen und Identity Manager-Umgebungen 35
Admin-Rollen und die -Benutzerkonsole 36
Erstellen von Admin-Rollen 36
Einführung in die Erstellung von Admin-Rollen 37
Definieren des Profils der Admin-Rolle 37
Auswählen von Admin-Aufgaben für die Rolle 38
Definieren von Mitgliederrichtlinien für Admin-Rollen 39
Definieren von Admin-Richtlinien für Admin-Rollen 40
Definieren von Eigentümerregeln für Admin-Rollen 41
Überprüfen von Admin-Rollen 41
Benutzern die Selbstzuweisung von Rollen gewähren 42

Kapitel 3: Admin-Aufgaben 43

Planen von Admin-Aufgaben....43
Beispiel einer Admin-Aufgabe....45
Verwendungsoptionen von Admin-Aufgaben....48
Standardmäßige Admin-Aufgaben....49
Erstellen von benutzerdefinierten Admin-Aufgaben....50
Definieren der Profile von Aufgaben....51
Registerkarte "Profil" beim Erstellen einer Admin-Aufgabe....51
Aufgaben-Konfigurationseigenschaften....55
Definieren von Aufgabenbereichen....56
Suchfensterkonfiguration....58
Auswählen von Registerkarten für Aufgaben....67
Registerkarte "Konten"....68
Registerkarte "Ablaufplan"....70
Anzeigen von Feldern in Aufgaben....71
Rollenverwendung anzeigen....71
Zuweisen von Workflow-Prozessen für Ereignisse....72
Verwalten eines Active Directory-Benutzerspeichers....72
Attribut "sAMAccountName"....72
Gruppentyp und Bereich....73
Externe Aufgaben für Anwendungsfunktionen....74
Die Registerkarte "Extern"....75
Die Registerkarte "Externe URL"....75
Erweiterte Aufgabenkomponenten....76
Erstellen von Business Logic Task-Handler....77
Admin-Aufgaben und Ereignisse....78
Primäre und sekundäre Ereignisse....79
Ereignisse für eine Aufgabe anzeigen....79
Für nicht geänderte Profile generierte Ereignisse....80
Verarbeiten von Admin-Aufgaben....80
Verarbeitung – synchrone Phase....81
Verarbeitung – asynchrone Phase....82
Bilder für Admin-Aufgaben....84

Kapitel 4: Benutzer 85

Erstellen und Konfigurieren von Benutzern....85
Erstellen und Konfigurieren eines Benutzers....87
Zuweisen einer Gruppe zu einem Benutzer....88
Weisen Sie einen Service direkt einem Benutzer zu....88
Weisen Sie einen Service einem Benutzer zu....89
Zulassen der Selbstregistrierung von Benutzern....90

Self-Service-Aufgaben 92
Zugriff auf Self-Service-Aufgaben 93
Einbetten eines Self-Service-Links in eine Unternehmens-Website 93
Mehrere Self-Service-Aufgaben konfigurieren 95
Einschränkung des Zugriffs auf die Rolle "Selbstverwaltung" 98

Kapitel 5: Kennwort-Management 99

Kennwort-Management in Identity Manager 99
Kennwortrichtlinien – Übersicht 100
Erstellen von Kennwortrichtlinien 101
Siehe Aktivieren zusätzlicher Kennwortrichtlinien. 101
Kennwortrichtlinien auf einen Benutzersatz anwenden 102
Konfigurieren des Kennwortablaufs 104
Konfigurieren der Kennwortzusammenstellung 107
Angeben regulärer Ausdrücke 109
Festlegen von Kennwortbeschränkungen 111
Konfigurieren erweiterter Kennwortoptionen 114
Kennwortrichtlinien verwalten 115
Kennwortrichtlinien und relationale Datenbanken 115
Kennwortkriterien für die CA IdentityMinder- und Siteminder-Integration 115
Zurücksetzen eines Kennworts oder Entsperren eines Kontos 116
Installieren von GINA oder Credential Provider 116
Konfigurieren von GINA 117
Konfigurieren des Credential Providers 120
Einstellungen in der Registrierung 122
Anpassen der "Powered By"-Meldung 127
Zurücksetzen eines Kennwortes für eine Windows-Anmeldung 128
Automatische GINA-Installation 128
Automatische Credential Provider-Installation 131

Kapitel 6: Synchronisieren von Kennwörtern auf Endpunkten 133

Kennwortsynchronisierung unter Windows 133
Kennwortsynchronisierung unter UNIX und Linux 144
Kennwortsynchronisierung auf OS400 159

Kapitel 7: Gruppen 169

Erstellen einer statischen Gruppe 169
Erstellen einer dynamischen Gruppe 170
Parameter für dynamische Gruppenabfragen 171
Erstellen von verschachtelten Gruppen 173

Beispiel für statische, dynamische und verschachtelte Gruppen 175
Gruppenadministratoren 176

Kapitel 8: Konten an verwalteten Endpunkten 179

Integrieren von verwalteten Endpunkten 180
Importieren der Rollendefinitions-Datei 181
Erstellen von Korrelationsregeln 181
Hinzufügen des Endpunkts zu der Umgebung 184
Erstellen einer Definition "Durchsuchen und Korrelieren" 184
Durchsuchen und Korrelieren des Endpunkts 186
Benutzer, Konten, und Rollen synchronisieren 187
Benutzer mit Rollen synchronisieren 189
Benutzer mit Kontovorlagen synchronisieren 190
Synchronisieren von Endpunkt-Benutzerkonten mit Kontovorlagen 191
Umgekehrte Synchronisierung mit Endpunktkonten 195
Funktionsweise der umgekehrten Synchronisierung 196
Zuordnen von Endpunktattributen 197
Richtlinien für die umgekehrte Synchronisierung 199
Erstellen einer Genehmigungsaufgabe für die umgekehrte Synchronisierung 204
Ausführen der umgekehrten Synchronisierung 206
Erweitern der benutzerdefinierten Attribute an Endpunkten 207
Kontoaufgaben 209
Endpunktkonten anzeigen oder ändern 209
Erstellen Sie ein bereitgestelltes Konto 211
Ausnahmenkonto erstellen 211
Zuweisen von verwaisten Konten 212
Zuweisen von Systemkonten 212
Aufgabenfenster "Konto verschieben" 213
Löschen eines Endpunktkontos 214
Ändern des Kennworts für ein Endpunktkonto 214
Durchführen von Aktionen auf mehrere Konten 215
Erweiterte Kontovorgänge 215
Ändern des globalen Benutzers für ein Konto 216
Funktionsweise der automatischen Durchsuchung 216
Löschen von Konten 217
Verwenden von "Löschen steht aus" 218
Wiederherstellen von gelöschten Konten 218

Kapitel 9: Bereitstellungsrollen 219

Bereitstellungsrollen und Kontovorlagen 219
Erstellen von Rollen zum Zuweisen von Konten 220

Kontovorlage erstellen 222
Erstellen einer Bereitstellungsrolle 223
Aufgaben im Zusammenhang mit Rollen und Vorlagen 224
Importieren einer Bereitstellungsrolle 224
Zuweisen von neuen Eigentümern für Bereitstellungsrollen 225
Kennwörter für von Bereitstellungsrollen erstellte Konten 225
Verarbeitungsreihenfolge von Ereignissen des Typs "Bereitstellungsrolle" 226
Aktivieren von geschachtelten Rollen in einer Umgebung 228
Aufnehmen einer Rolle in eine Bereitstellungsrolle 229
Attribute in Kontovorlagen 229
Funktions- und anfängliche Attribute 230
Regelzeichenfolgen für Attribute 231
Werte für Attribute 233
Erweiterte Regelausdrücke 233
Verschmelzen von Regelzeichenfolgen und Werten 234
Untergeordnete Zeichenfolgen für Regeln 234
Regelausdrücke mit mehreren Werten 235
Explizite Regeln für globale Benutzerattribute 237
Integrierte Regelfunktionen 238
Leistung von Bereitstellungsrollen 240
JIAM-Objekt-Cache 240
Sitzungspools 242
Provisionierung von Aufgaben für vorhandene Umgebungen 242

Kapitel 10: Verwaltete Services (Basiszugriffsanfragen) 243

Erstellen von Services 244
Wissenswertes über die Service-Erstellung 246
Einführung in die Service-Erstellung 247
Definieren des Service-Profils 247
Definieren der Admin-Richtlinien für den Service 249
Definieren der Eigentümerregeln für den Service 250
Definieren der Voraussetzungen für den Service 250
Konfigurieren der E-Mail-Benachrichtigung für die Service-Erneuerung 251
Wissenswertes über Abwicklungs- und Annulierungsaktionen 252
Definieren der Abwicklungs- und Annulierungsaktionen für den Service 252
Weisen Sie einen Service einem Benutzer zu. 254
Servicezuweisung bestätigen 255
Services für Benutzer verfügbar machen 255
Weisen Sie einen Service einem Benutzer zu. 257
Servicezuweisung bestätigen 258
Einen Service ändern 259

Einen Service löschen 261
Servicemitglieder überprüfen und entfernen 262
Einen Service löschen 262
Erneuern des Zugriffs auf Services 263

Kapitel 11: Synchronisierung 265

Benutzersynchronisierung zwischen Servern 265
Eingehende Synchronisierung 265
Failover für eingehende Synchronisierung 265
Ausgehende Synchronisierung 265
Enable Password Synchronization (Kennwortsynchronisierung ermöglichen) 267
Synchronisieren von Benutzern in Aufgaben zum Erstellen oder Ändern von Benutzern 268
Synchronisierungsaufgaben 269
Gründe, warum Benutzer nicht mehr synchronisiert sind 271
Benutzersynchronisierung 271
Synchronisierung von Kontovorlagen 274
Kontosynchronisierung 278

Kapitel 12: Workflow 281

Workflow-Übersicht 281
WorkPoint-Prozessdiagramm 282
Workflow und E-Mail-Benachrichtigung 282
WorkPoint-Dokumentation 283
Workflow-Steuermethoden 283
Verwenden der Workflow-Kontrolle - Vorlagenmethode 284
Voraussetzung: Workflow aktivieren 285
Stellen von Admin-Aufgaben unter Workflow-Kontrolle - Vorlagenmethode 285
Aufgaben- oder ereignisbasierter Workflow 286
Prozessvorlagentypen 293
Arten von Teilnehmer-Resolver 297
Festlegen einer E-Mail-Richtlinie für einen Workflow-Prozess 302
Workflow-Beispiel: Benutzer erstellen 302
Verwenden der WorkPoint-Methode 304
Konfigurieren der Verwaltungstools von WorkPoint 306
WorkPoint-Prozesse 311
Workflow-Aktivitäten 317
Teilnehmer-Resolver: WorkPoint-Methode 319
Prozesse im WorkPoint Designer 330
Job- und Prozessinstanzen 333
Workflow-Aktivitäten ausführen 335
Der Workflow-Server schließt die Aktivität ab. 336

Workpoint-Job-Ansicht 337
Hinzufügen der Registerkarte "Job anzeigen" zu den vorhandenen Registerkarten für Genehmigungen 338
Anzeigen der Registerkarte "Job anzeigen" für eine Genehmigungsaufgabe 339
Anzeigen eines Workflow-Jobs für Workflows auf Ereignisnebene 339
Anzeigen eines Workflow-Jobs für Workflows auf Aufgabenebene 340
Richtlinienbasierter Workflow 340
Standard-Workflow-Prozesse 341
Regelobjekte 342
Regelauswertung 343
Richtlinienreihenfolge 345
Richtlinienbeschreibung 347
Hervorheben geänderter Attribute in Genehmigungsfenstern 348
Genehmigungsrichtlinien und mehrwertige Attribute 349
Attribute werden auf Workflow-Genehmigungsfenstern als geändert hervorgehoben 350
Richtlinienbeispiele 350
Konfigurieren des richtlinienbasierten Workflows für Ereignisse 353
Konfigurieren des richtlinienbasierten Workflows für Aufgaben 355
Konfigurieren einer Genehmigungsrichtlinie 356
Status des richtlinienbasierten Workflows 357
Globale, richtlinienbasierte Workflow-Zuordnung auf Ereignisebene 358
Online-Anfragen 362
Online-Anfrage-Aufgaben 362
Online-Anfrageprozess 364
Verlauf der Online-Anfrage 365
Verwenden von Online-Anfragen 365
Schaltflächen für Workflow-Aktionen 366
Workflow-Schaltflächen in Genehmigungsaufgaben 367
Schaltflächenkonfiguration in CA IdentityMinder 367
Hinzufügen von Workflow-Aktionsschaltflächen 368
Arbeitslisten und Arbeitselemente 371
Anzeigen einer Arbeitsliste 372
Reservieren von Arbeitselementen 373
Delegieren von Arbeitselementen 374
Neuzuweisen von Arbeitselementen 380
Massenvorgänge für Arbeitselemente 383

Kapitel 13: E-Mail-Benachrichtigungen 385

E-Mail-Benachrichtigungen in CA IdentityMinder 386
Auswählen einer E-Mail-Benachrichtigungsmethode 387
Konfigurieren vom SMTP-Einstellungen 388
Konfigurieren von SMTP-Einstellungen auf JBoss 389

Konfigurieren von SMTP-Einstellungen auf WebLogic 390
Konfigurieren von SMTP-Einstellungen auf WebSphere 390
Erstellen von E-Mail-Benachrichtigungsrichtlinien 391
Registerkarte "Profil" für E-Mail-Benachrichtigungen 392
Registerkarte "Sendezeitpunkt" 393
Registerkarte "Empfänger" 395
Inhalt 396
Ändern von E-Mail-Benachrichtigungsrichtlinien 398
Deaktivieren von E-Mail-Benachrichtigungsrichtlinien 399
Anwendungsfall: Senden einer Begrüßungs-E-Mail 400
Verwenden von E-Mail-Vorlagen 401
Aktivieren von E-Mail-Benachrichtigungen 402
Konfigurieren von Ereignissen oder Aufgaben, bei denen E-Mails gesendet werden 402
E-Mail-Inhalt 404
E-Mail-Vorlagen 405
Erstellen von E-Mail-Vorlagen 408
Benutzerdefinierte E-Mail-Vorlagen 408
Bereitstellung von E-Mail-Vorlagen 428

Kapitel 14: Berichterstellung 431

Übersicht 431
Bericht-Prozess 433
So führen Sie einen Snapshot-Bericht aus 434
Berichtsserver-Verbindung konfigurieren 437
Erstellen einer Snapshot-Datenbankverbindung 438
Erstellen einer Snapshot-Definition 439
Beispiel: Erstellen einer Snapshot-Definition für Benutzerberechtigungsdaten 441
Snapshots verwalten 442
Snapshot-Daten erfassen 442
Einer Berichtsaufgabe eine Snapshot-Definition zuweisen 445
Bericht anfordern 446
Anzeigen des Berichts 448
So führen Sie einen Nicht-Snapshot-Bericht aus 449
Berichtsserver-Verbindung konfigurieren 450
Erstellen einer Verbindung für den Bericht 451
Zuweisen einer Verbindung zu einer Berichtsaufgabe 451
Bericht anfordern 452
Anzeigen des Berichts 454
Festlegen von Berichtsoptionen 455
So können Sie einen benutzerdefinierten Snapshot-Bericht erstellen und ausführen 456
Erstellen von Berichten in Crystal Reports Developer 458

Erstellen der XML-Datei mit den Berichtsparametern 458
Hochladen des Berichts und der XML-Datei mit den Berichtsparametern 463
Erstellen der Berichtsaufgabe 465
Bericht anfordern 468
Anzeigen des Berichts 470
Fehlerbehebung 470
Beim Anzeigen eines Berichts wird der Benutzer zur Infoview-Anmeldeseite weitergeleitet 471
Generieren von Benutzerkonten für mehr als 20.000 Datensätze 471

Kapitel 15: Identitätsrichtlinien 473

Identitätsrichtlinien 473
Arbeitsblatt zum Planen von Identitätsrichtliniensätzen 474
Erstellen eines neuen Identitätsrichtliniensatzes 475
Verwalten eines neuen Identitätsrichtliniensatzes 487
Synchronisieren von Benutzern und Identitätsrichtlinien 488
Identitätsrichtliniensätze in einer Identity Manager-Umgebung 492
Präventive Identitätsrichtlinien 497
Aktionen für Verletzungen präventiver Identitätsrichtlinien 498
Funktionsweise von präventiven Identitätsrichtlinien 499
Wichtige Hinweise zu präventiven Identitätsrichtlinien 500
Erstellen einer präventiven Identitätsrichtlinie 501
Anwendungsfall: Verhindern, dass Benutzer widersprüchliche Rollen besitzen 502
Workflow und präventive Identitätsrichtlinien 503
Kombinieren von Identitätsrichtlinien und präventiven Identitätsrichtlinien 508

Kapitel 16: Policy Xpress 511

Übersicht über Policy Xpress 511
Erstellen einer Richtlinie 512
Profil 513
Ereignisse 517
Datenelemente 518
Eintrittsregeln 521
Aktionsregeln 522
Erweitert 527

Kapitel 17: Mobile CA IdentityMinder-App 529

Funktionsweise der Implementierung 530
So konfigurieren Sie CA IdentityMinder zur Unterstützung mobiler Apps 531
Konfigurieren von erforderlichen Attributen 532
Importieren von Admin-Aufgaben 534

Erstellen einer Webservices-Konfiguration 535
Ändern der Registrierungs-E-Mail 536
Konfigurieren einer mobilen App 537
Download der mobilen App 539
Fehlerbehebung bei mobilen Apps 540

Kapitel 18: CA Berichte zu Benutzeraktivitäten 541

CA Enterprise Log Manager-Funktionen 541
CA Enterprise Log Manager-Komponenten 542
Beschränkungen bei der Integration 542
Integrieren von CA Enterprise Log Manager mit CA IdentityMinder 542
Integrieren von zusätzlichen CA Enterprise Log Manager-Berichten oder -Abfragen mit CA Identity Manager 553
Registerkarte "Konfigurieren der Enterprise Log Manager-Viewer" 554

Kapitel 19: Zugriffsrollen 557

So verwalten Zugriffsrollen Berechtigungen 558
Beispiel: Indirekte Änderung eines Profilattributs 558
Erstellen einer Zugriffsrolle 559
Beginnen Sie mit der Erstellung einer Zugriffsrolle 559
Definieren des Profils für Zugriffsrollen 560
Definieren von Mitgliederrichtlinien für Zugriffsrollen 560
Definieren Sie Admin-Richtlinien für Zugriffsrollen 561
Definieren von Eigentümerregeln für Zugriffsrollen 561

Kapitel 20: Systemaufgaben 563

Standardsystemaufgaben 563
Hinzufügen von Benutzern mit einer Feeder-Datei 564
Hinweise zum Massendatenlader 565
Erstellen von Feeder-Dateien 568
Registerkarte "Details der Loader-Datensätze" 569
Registerkarte "Zuordnung der Loader-Aktionen" 570
Registerkarte "Laderbenachrichtigungs-Details" 571
Bestätigen von Änderungen in der Massendatenlader-Aufgabe 571
Konfigurieren von E-Mail-Benachrichtigungen für Massendatenlader-Aufgaben 573
Planen der Aufgabe "Massendatenlader" 573
Ändern der Parser-Datei für den Massendatenlader 573
Webservice-Unterstützung für den Massendatenlader 574
JDBC-Verbindungsverwaltung 575
JDBC-Verbindung erstellen 575

Logical-Attribute-Handler 575
Erstellen von Logical-Attribute-Handlern 576
Kopieren von Logical-Attribute-Handlern 577
Erstellen des Logical-Attribute-Handler "ForgottenPasswordHandler" 577
Löschen von Logical-Attribute-Handlern 578
Ändern von Logical-Attribute-Handlern 578
Anzeigen von Logical-Attribute-Handlern 579
Auswahlfelddaten 579
Aufgabenfenster "Korrelationsattribute konfigurieren" 580
Aufgabenfenster "Auf globaler Richtlinie basierter Workflow für Ereignisse konfigurieren" 581
Aufgabenstatus in CA IdentityMinder 582
So legt CA IdentityMinder den Aufgabenstatus fest 583
Gesendete Aufgaben anzeigen 584
Registerkarte "Benutzerverlauf" 595
Bereinigen gesendeter Aufgaben 600
Registerkarte "Wiederholungen" 601
Registerkarte "Gesendete Aufgaben bereinigen" 604
Löschen wiederkehrender Aufgaben 604
Konfigurieren der Enterprise Log Manager-Verbindung 605
Löschen der Enterprise Log Manager-Verbindung 606
Geheime Schlüssel verwalten 607

Kapitel 21: Aufgabenpersistenz 609

Automatisierte Aufgaben-Persistenz-Bereinigung und -Archivierung 609
Registerkarte "Wiederholungen" 610
Registerkarte "Gesendete Aufgaben bereinigen" 611
Sofortiges Ausführen eines Jobs 612
Planen eines neuen Jobs 612
Ändern eines vorhandenen Jobs 613
Löschen einer wiederkehrenden Aufgabe 613
Migrieren der Aufgabenpersistenz-Datenbank 614
Aktualisieren der Datei "tpmigration125.properties" 615
Festlegen der JAVA_HOME-Variable 615
Ausführen des runmigration-Tools 616

Kapitel 1: Planen von Rollen

Bei der Planung der Rollen entscheiden Sie, welche Art von Rollen Ihr Geschäft oder Ihre Organisation benötigt und wie die Verwaltung von Benutzern und ihr Zugriff auf Anwendungen delegiert werden soll. Basierend auf diesen Entscheidungen bestimmen Sie die Merkmale jeder Rolle.

Für eine effektive Verwendung von Rollen müssen die folgenden Arten von Fragen zu den Anforderungen der Benutzer und den Zuständigkeiten der Administratoren berücksichtigt werden:

- In welchen Abteilungen und Organisationen sind Benutzer zu verwalten?
- Welche zusätzlichen Konten in verwalteten Endpunkten werden von den Benutzern benötigt?
- Welche Benutzer sollten Administratoren von anderen Benutzern sein?
- Wer sollte die Administratoren verwalten?
- Welcher Admin- und Zugriffsaufgaben werden in jeder Rolle benötigt?
- Wer sollte Rollen und Aufgaben erstellen?
- Wie kann ich Rollen verwenden, um Arbeit zu delegieren?

  Die letzte Frage betrifft die Aufteilung der Verwaltung von Benutzern und Erteilung von Zugriff auf Anwendungen. Weitere Informationen zum Delegierungsmodell finden Sie unter Delegierte Verwaltung.

Basierend auf den Antworten auf diese Fragen können Sie festlegen, wie viele und welche Art von Rollen benötigt werden.

Dieses Kapitel enthält folgende Themen:

Entscheidungen in Bezug auf Rollen (siehe Seite 17)
Zweck der Rollen (siehe Seite 18)
Erstellen von zusätzlichen Administratoren (siehe Seite 19)
Rollenmerkmale (siehe Seite 23)
Checkliste für die Rollenplanung (siehe Seite 33)

Entscheidungen in Bezug auf Rollen

Im folgenden Abschnitt finden Sie Informationen, die Ihnen dabei helfen, informierte Entscheidungen bezüglich Rollen zu treffen.

Zweck der Rollen

Für eine effektive Verwendung von Rollen müssen die folgenden Arten von Fragen zu den Anforderungen der Benutzer und den Zuständigkeiten der Administratoren berücksichtigt werden:

- In welchen Abteilungen und Organisationen sind Benutzer zu verwalten?
- Welche zusätzlichen Konten in verwalteten Endpunkten werden von den Benutzern benötigt?
- Welche Benutzer sollten Administratoren von anderen Benutzern sein?
- Wer sollte die Administratoren verwalten?
- Welcher Admin- und Zugriffsaufgaben werden in jeder Rolle benötigt?
- Wer sollte Rollen und Aufgaben erstellen?
- Wie kann ich Rollen verwenden, um Arbeit zu delegieren?

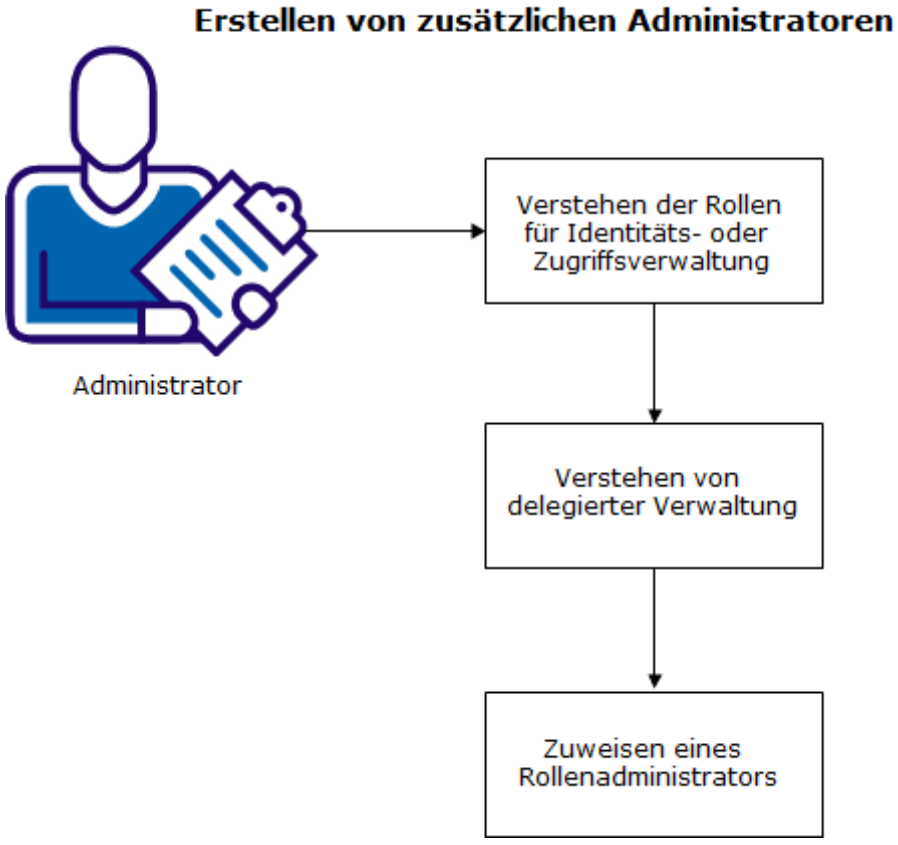
  Die letzte Frage betrifft die Aufteilung der Verwaltung von Benutzern und Erteilung von Zugriff auf Anwendungen. Weitere Informationen zum Delegierungsmodell finden Sie unter Delegierte Verwaltung.

Basierend auf den Antworten auf diese Fragen können Sie festlegen, wie viele und welche Art von Rollen benötigt werden.

Erstellen von zusätzlichen Administratoren

Sie können als Einziger dafür verantwortlich sein, den Benutzern in Ihrem System alle Rollen zuzuweisen. Sie können die Aufgabe des Zuweisens von Benutzerrollen auch mit anderen teilen, indem Sie zusätzliche Administratoren festlegen. Diese Vorgehensweise wird *delegierte Verwaltung* genannt.

Das folgende Diagramm zeigt die erforderlichen Informationen und die durchzuführenden Schritte beim Erstellen von zusätzlichen Administratoren.



In den folgenden Themen wird beschrieben, wie zusätzliche Administratoren erstellt werden:

- Rollen für Identitäts- oder Zugriffsmanagement (siehe Seite 20)
- Delegierte Verwaltung (siehe Seite 20)
- Festlegen eines Rollenadministrators (siehe Seite 21)

Rollen für Identitäts- oder Zugriffsmanagement

Für das Management von Benutzeridentitäten und des Zugriffs auf andere Konten stellt CA CloudMinder zwei Arten von Rollen bereit. Mit einer Admin-Rolle kann ein Benutzer andere Benutzer verwalten und zum Beispiel ein Benutzerkennwort oder die Gruppenmitgliedschaft ändern. Admin-Rollen können auch jede Aufgabe einschließen, die in der Benutzerkonsole angezeigt wird. Mit einer Bereitstellungsrolle hat ein Benutzer Zugriff auf andere Unternehmensanwendungen, zum Beispiel ein E-Mail-System.

Weitere Details zu Rollen werden in der folgenden Tabelle beschrieben:

Art der Rolle	Zweck
Admin-Rolle	Umfasst Admin-Aufgaben, die ein Benutzer, dem diese Rolle zugewiesen wurde, in CA CloudMinder durchführen kann, zum Beispiel Aufgaben für die Verwaltung von Benutzern.
Bereitstellungsrolle	Umfasst Kontovorlagen, die Konten definieren, die in verwalteten Endpunkten, zum Beispiel einem E-Mail-System, vorhanden sind. Die Kontovorlagen definieren auch, wie Benutzerattribute diesen Konten zugeordnet werden.
Zugriffsrolle	Zugriffsrollen bieten eine zusätzliche Möglichkeit, Berechtigungen in CA IdentityMinder oder einer anderen Anwendung anzugeben. Sie können Zugriffsrollen z. B. für die folgenden Aktionen verwenden: ■ Angeben von indirektem Zugriff auf ein Benutzerattribut ■ Erstellen komplexer Ausdrücke ■ Festlegen eines Profilattributs, das eine andere Anwendung für die Bestimmung von Berechtigungen verwenden kann

Delegierte Verwaltung

Mit delegierter Verwaltung wird die Verwendung von Rollen bezeichnet, um die Aufgabe der Verwaltung von Benutzern und des Erteilens von Zugriff auf Anwendungen zu teilen.

Für jede Rolle im System kann ein Benutzer eine oder mehrere der folgenden Funktionen innehaben:

Funktion	Definition
Rolleneigentümer	Ändert die Rolle.
Rollenadministrator	Weist die Rolle Benutzern und anderen Rollenadministratoren zu.

Funktion	Definition
Rollenmitglied	Verwendet die Rolle, um Admin- oder Zugriffsaufgaben auszuführen oder ein Endpunktkonto zu verwenden.

Indem Sie diese Funktionen auf andere Benutzer verteilen, können Sie die Aufgabe der Verwaltung einer Rolle teilen. Zum Beispiel können Administratoren mit einer geringeren Berechtigungsstufe Rollenmitgliedschaften verwalten und Administratoren mit einer höheren Berechtigungsstufe Rollen ändern.

Sie können die delegierte Verwaltung folgendermaßen implementieren:

- Legen Sie einen Benutzer direkt als Administrator für eine bestimmte Rolle fest.
- Konfigurieren Sie *Admin-Regeln* für eine Rolle. Admin-Regeln definieren, welche Benutzer Administratoren einer Rolle sein können. Das System erstellt automatisch zusätzliche Administratoren, wenn Benutzer den angegebenen Kriterien in den Regeln entsprechen.

  Hinweis: Nur ein Administrator mit den Berechtigungen, eine Rolle zu ändern, kann Admin-Regeln für diese Rolle konfigurieren. Normalerweise führen Systemadministratoren diese Aktivität aus. Informationen zum Konfigurieren von Admin-Regeln, die die Verwaltung für eine Rolle automatisch delegieren, finden Sie im Abschnitt "Admin-Rollen" in den Verweisinformationen der Online-Hilfe.

Festlegen eines Rollenadministrators

Sie können einen Benutzer als Administrator einer Rolle festlegen. Der Administrator kann die Rolle dann anderen Benutzern zuweisen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole als Benutzer mit Rollenverwaltungsaufgaben an.
2. Wählen Sie die Option "Rollen und Aufgaben" aus.
3. Wählen Sie eine der folgenden Aufgaben aus:
   - Admin-Rollen, Mitglieder/Administratoren von Admin-Rolle ändern
   - Bereitstellungsrollen, Mitglieder/Administratoren von Bereitstellungsrolle ändern
   - Zugriffsrollen, Mitglieder/Administratoren von Zugriffsrolle ändern

   Ein Suchfenster wird geöffnet.
4. Wählen Sie die Rolle aus, die Sie dem Benutzer zuweisen möchten.
5. Klicken Sie auf die Registerkarte "Administratoren".

   Eine Liste mit aktuellen Rollenadministratoren wird angezeigt.

6. Klicken Sie auf "Einen Benutzer hinzufügen".

   Ein Suchfenster wird geöffnet.

7. Suchen Sie nach dem Benutzer, den Sie als Administrator hinzufügen möchten, und klicken Sie auf "Auswählen".

   Eine aktualisierte Liste mit Rollenadministratoren wird angezeigt.

8. Klicken Sie auf "Senden".

   Der Benutzer wird ein Administrator der Rolle. Dieser Schritt schließt den Vorgang ab, mit dem die Verwaltung einer Bereitstellungsrolle delegiert wird. Der Administrator kann die Rolle jetzt anderen Benutzern zuweisen und Zugriff auf die zugeordneten Endpunktkonten erteilen.

Delegierungsschritte

Nachdem Sie die Verwendung der Rollen basierend auf dem Zweck der Rollen festgelegt haben, wird die delegierte Verwaltung folgendermaßen durchgeführt:

1. Ein Administrator erstellt die Rolle mit Regeln, die festlegen, wer ein Rolleneigentümer, Rollenadministrator oder Rollenmitglied ist.
2. Ein Rolleneigentümer ändert die Rolle, wenn Änderungen erforderlich sind.
3. Ein Rollenadministrator:
   - Weist weitere Rollenadministratoren zu (optional).
   - Weist weitere Rollenmitglieder zu (optional).

   Einige Benutzer sind bereits Rollenadministratoren oder -mitglieder, da sie den in der Rolle definierten Regeln entsprechen.
4. Ein Rollenmitglied verwendet die Rolle:
   - Ein Mitglied der Admin-Rolle verwaltet Benutzer und andere Objekte in der Identity Manager-Umgebung.
   - Ein Zugriffsrollenmitglied führt Funktionen in Unternehmensanwendungen aus.
   - Ein Mitglied der Bereitstellungsrolle verwendet die von Richtlinien in der Rolle definierten Konten.

Delegierungsbeispiel

Sie können eine Rolle mit Regeln erstellen, die festlegen, wer ein Mitglied oder Administrator sein kann. Sie können die Rolle dann zuweisen, sodass andere Benutzer (die nicht bereits den Regeln entsprechen) ein Rollenmitglied oder Rollenadministrator werden können.

Betrachten Sie das folgende Beispiel für Administratoren, die die Rechte von Endbenutzern bezüglich Unternehmensanwendungen verwalten:

- Jeff ist ein Rolleneigentümer für die Rolle "Buchhalter"; und wenn die Rolle Änderungen erfordert, ändert Jeff die Rolle.
- David und Lisa sind Rollenadministratoren für diese Rolle. Sie weisen regionale Benutzer als Rollenmitglieder zu.
- Andere Benutzer sind Rollenmitglieder, ohne dass sie als Rollenmitglieder zugewiesen wurden. Sie sind Rollenmitglieder, weil sie der Regel entsprechen.

  Die Rollenmitglieder verwenden die Rolle "Buchhalter", um Aufträge zu generieren und andere Aufgaben in Finanzanwendungen auszuführen.

Im Abschnitt Rollenmerkmale finden Sie Details zu Regeln und anderen Merkmalen einer Rolle.

Rollenmerkmale

Wenn Sie eine Rolle erstellen, definieren Sie die in der folgenden Tabelle angezeigten Merkmale:

Merkmale	Definition
Rollenprofil	Allgemeine Merkmale der Rolle.
Aufgaben	Aufgaben für eine Admin-Rolle.
Kontovorlagen	Vorlagen, die Konten in verwalteten Endpunkten für eine Bereitstellungsrolle definieren.
Mitgliederregeln, Mitgliederrichtlinien	Eine Mitgliederregel definiert Bedingungen dafür, dass ein Benutzer ein Mitglied einer Zugriffs- oder Admin-Rolle ist. Eine Mitgliederrichtlinie verbindet eine Mitgliederregel mit Bereichsregeln. **Hinweis:** Bereitstellungsrollen haben keine Mitgliederregeln und Richtlinien. Um einen Benutzer zu einem Mitglied zu machen, verwenden Sie "Mitglieder/Administratoren von Bereitstellungsrolle ändern".

Merkmale	Definition
Admin-Regeln, Admin-Richtlinien	■ Eine Admin-Regel legt die Bedingungen fest, unter denen ein Benutzer ein Rollen-Administrator ist. ■ Eine Admin-Richtlinie verbindet eine Admin-Regel mit einer Bereichsregel und Administratorrechten für das Zuweisen der Rolle.
Eigentümerregeln	Bedingungen, unter denen ein Benutzer ein Rolleneigentümer ist.
Bereichsregeln	Limits dafür, welche Objekte von der Rolle verwaltet werden können.
Aktionen hinzufügen Entfernaktionen	Wechselt zu einem Benutzerprofil, wenn ein Benutzer als Rollenmitglied oder Administrator hinzugefügt oder entfernt wird.

Rollenprofil

Das Rollenprofil ist der Name und die Beschreibung der Rolle und legt fest, ob die Rolle aktiviert ist. Wenn aktiviert, kann die Rolle sofort nach der Erstellung verwendet werden.

Aufgaben für die Rolle

Für eine Admin-Rolle können Sie Admin-Aufgaben, einschließlich externer Aufgaben, aus einer oder mehreren Kategorien wählen.

Kontovorlagen

Jede Bereitstellungsrolle enthält Kontovorlagen. Sie definieren die Konten, die in verwalteten Endpunkten vorhanden sind. Zum Beispiel könnte ein Endpunkt für ein Exchange-Konto die Größe des Postfachs definieren. Kontovorlagen definieren auch, wie Benutzerattribute Konten zugeordnet werden.

Sie können für jeden Endpunkttyp einen oder mehrere Endpunkte wählen. Ein Benutzer, dem die Rolle zugewiesen wird, erhält ein Konto im Endpunkt.

Mitglieder-, Admin- und Eigentümerregeln

Jede Rolle umfasst Regeln dazu, welche Benutzer Mitglieder, Administratoren oder Eigentümer der Rolle werden können. Daher kann ein Benutzer Mitglied einer Rolle, mehrerer Rollen oder keiner Rolle sein.

Mitglieder-, Admin- und Eigentümerregeln verwenden die Bedingungen in der folgenden Tabelle:

Regelbedingung	Beispiel	Regelsyntax
Der Benutzer muss einem Attributwert entsprechen.	Benutzer wobei Titel beginnt mit Senior	wobei <Benutzerfilter>
Der Benutzer muss mehreren Attributwerten entsprechen.	Benutzer wobei Titel=Manager und Standort=Ost	wobei <Benutzerfilter>
Der Benutzer muss den bezeichneten Organisationen angehören.	Benutzer in Organisation Vertrieb und niedriger	in <Org-Regel>
Der Benutzer muss Organisationen angehören, die eine Bedingung erfüllen, welche von den Attributen der Organisation festgelegt wird.	Benutzer in Organisation wobei Geschäftstyp=Gold oder Platin	in Organisation wobei <Org-Filter>
Der Benutzer muss bestimmten Organisationen angehören, und er muss bestimmten Benutzerattributen entsprechen.	Benutzer wobei Titel=Manager und Standort=Ost und sind in Organisation Vertrieb oder Marketing	wobei <Benutzerfilter> und sind in <Org-Regel>
Der Benutzer muss einer bestimmten Gruppe angehören.	Benutzer als Mitglieder von 401K Gruppe	als Mitglieder von <Gruppe> Gruppe
Der Benutzer muss Mitglied der Rolle sein.	Benutzer als Mitglieder von Helpdesk Rolle	als Mitglieder von <Rollenregel>
Der Benutzer muss Administrator einer Rolle sein.	Benutzer als Administratoren von Vertriebs-Manager Rolle	als Administratoren von <Rollenregel>
Der Benutzer muss Eigentümer einer Rolle sein.	Benutzer als Eigentümer von Benutzer-Manager Rolle	als Eigentümer von <Rollenregel>
Der Benutzer muss einer Gruppe angehören, die eine Bedingung erfüllt, welche von den Attributen der Gruppe festgelegt werden.	Benutzer als Mitglieder von Gruppen, bei denen Eigentümer=CIO	als Mitglieder von <Gruppenfilter>

Regelbedingung	Beispiel	Regelsyntax
Der Benutzer muss eine Bedingung auf Grundlage einer LDAP-Anfrage erfüllen.	(In Situationen, in denen eine in der Benutzerkonsole von Identity Manager erstellte Abfrage unzureichend ist, verwenden Sie ein LDAP-Verzeichnis)	Benutzer von der Abfrage zurückgegeben ldap_query

Manche Regeln erfordern möglicherweise den Vergleich eines Werts mit einem mehrwertigen Attribut. Damit die Regel zutrifft, muss mindestens ein Wert des mehrwertigen Attributs die Regel erfüllen. Wenn die Regel beispielsweise "Attribute A EQUALS 1" lautet und Attribut A für Benutzer X den Wert "1, 2, 3" hat, erfüllt Benutzer X das Kriterium.

Der Benutzer, der die Rolle erstellt, kann sie möglicherweise nicht ändern. Um die Rolle ändern zu können, muss der Benutzer die Bedingungen in den Eigentümerregeln erfüllen.

Hinweis: In umfangreichen Implementierungen kann die Auswertung von Mitglieder-, Admin- und Eigentümerregeln erhebliche Zeit in Anspruch nehmen. Sie können die Auswertungszeit für Regeln mit Benutzerattributen verkürzen, indem Sie die Option für die Auswertung im Arbeitsspeicher aktivieren. Weitere Informationen finden Sie im *Konfigurationshandbuch*.

Bereichsregeln

Sie verbinden Mitglieder- und Admin-Regeln mit Bereichsregeln. *Bereichsregeln* beschränken Objekte, auf denen die Rolle verwendet werden kann.

- Für ein Rollenmitglied steuern Bereichsregeln, welche Objekte mit der Rolle verwaltet werden können.
- Für einen Rollenadministrator steuern Bereichsregeln, welche Benutzer Rollenmitglieder und Administratoren werden können.

Der Bereich bezieht sich auf das primäre Objekt der Aufgabe. Zum Beispiel ist der Benutzer das primäre Objekt der "Benutzer erstellen"-Aufgabe. Allerdings bezieht sich der Bereich nicht auf die Gruppen für diesen Benutzer, da eine Gruppe ein sekundäres Objekt ist.

Für die meisten Objekttypen können Sie die Typen der Bereichsregeln in folgender Tabelle angeben.

Regelbedingung	Beispiel	Regelsyntax
Alle	Rollenmitglieder können alle Objekte verwalten	Alle
Das Objekt muss mit einem oder mehreren Attributwerten übereinstimmen.	Benutzer wobei **Titel** beginnt mit **Senior**	wo <filter>

Wenn Sie die Filteroption auswählen, zeigt CA IdentityMinder zwei Typen von Filtern an:

<attribut> <komparator><wert>

Ein Attribut im Profil des Objekts muss mit einem bestimmten Wert übereinstimmen.

<attribute> <komparator> admins <Benutzerattribute>

Ein Attribut im Profil des Objekts muss mit einem Attribut auf dem Profil des Administrators übereinstimmen. Zum Beispiel: Benutzer, bei denen Manager = Benutzer-ID des Admins ist.

Zusätzliche Optionen, die in den folgenden Tabellen beschrieben werden, sind für Benutzer, Gruppe und Organisationsobjekte verfügbar.

Hinweis: Folgende Benutzerbereichsregeln sind Beispiele. Sie können andere Regeln erstellen, um verschiedene Beziehungen zwischen dem Administrator und den Benutzern zu verarbeiten, die der Administrator verwalten kann.

Regelbedingung	Beispiel	Regelsyntax
Der Benutzer muss einem Attributwert entsprechen.	Benutzer, bei denen Mitglieder der Gruppenverkäufe oder Mobiltelefon nicht gleich Null ist	wobei <Benutzerfilter>
Der Benutzer muss mehreren Attributwerten entsprechen.	Benutzer, bei denen Titel=Manager und Standort=USA ist	wobei <Benutzerfilter>

Regelbedingung	Beispiel	Regelsyntax
Der Benutzer muss den bezeichneten Organisationen angehören.	Benutzer in Organisation "Australien" oder "Neuseeland" **Hinweis:** Die Bereichsregel "Organisation" bezieht sich auf Unterorganisationen der Organisation, die der Regel entspricht. Wenn z. B. die Organisationsregel "in Organization1" ist, dann bezieht sich die Bereichsregel auf "Organization1.1" und "Organization1.2", jedoch nicht auf "Organization1".	in <Org-Regel>
Der Benutzer muss Organisationen angehören, die eine Bedingung erfüllen, welche von den Attributen der Organisation festgelegt wird.	Benutzer in Organisation wobei Geschäftstyp=Gold oder Platin	in Organisation wobei <Org-Filter>
Der Benutzer muss bestimmten Organisationen angehören, und er muss bestimmten Benutzerattributen entsprechen.	Benutzer, bei denen Titel=Manager und Standort=Ost ist, und Benutzer, die in der Organisation "Vertrieb" oder "Marketing" sind	wobei <Benutzerfilter> und sind in <Org-Regel>
Das Attribut auf dem Profil eines Benutzers muss mit einem Attribut auf dem Profil des Administrators übereinstimmen.	Benutzer, bei denen Manager = Benutzer-ID des Admins ist	wobei <Benutzerattribut> <Komparator> <Benutzerattribut> des Admins **Hinweis:** Verwenden Sie nicht den "Ungleich"-Komparator mit einem mehrwertigen Attribut.
Der Benutzer ist in der gleichen Organisation wie der Administrator.	Benutzer in der Organisation, bei der "Jeff" (der Administrator) ein Mitglied ist	Die Organisation des Admins
Der Benutzer ist in einer Organisation, die auf dem Attribut des Administrators aufgelistet ist.	Benutzer im Vertrieb oder Marketing	Organisation, die ein Wert im <Admin-Attr> des Admins ist

Hinweis: Folgende Gruppenbereichsregeln sind nur Beispiele. Sie können andere Regeln erstellen, um verschiedene Beziehungen zwischen dem Administrator und den Gruppen zu verarbeiten, die der Administrator verwalten kann.

Regelbedingung	Beispiel	Regelsyntax
Die Gruppe muss einem Attributwert entsprechen.	Gruppenname, bei dem der Gruppenname = 401K ist	wobei <Gruppenfilter>
Die Gruppen müssen den benannten Organisationen angehören.	Gruppen in der Organisation "Abrechnung" und niedriger	in <Org-Regel>
Die Gruppe muss mit einem Attributwert übereinstimmen und den benannten Organisationen angehören.	Gruppen, bei denen "BusinessType = finance" sind und die in der Organisation "Vertrieb" und niedriger sind	wobei <Gruppenfilter> und sind in <Org-Regel>
Die Gruppe muss in einem Attribut des Administrators aufgelistet sein.	Gruppen, bei denen Beschreibung = Engineering ist	wobei <Gruppenattribut> <Komparator> <Benutzerattribut> des Admins **Hinweis:** Verwenden Sie nicht den "Ungleich"-Komparator mit einem mehrwertigen Attribut.

Hinweis: Folgende Organisationsbereichsregeln sind nur Beispiele. Sie können andere Regeln erstellen, um verschiedene Beziehungen zwischen dem Administrator und den Organisationen zu verarbeiten, die der Administrator verwalten kann.

Regelbedingung	Beispiel	Regelsyntax
Die Organisation muss einem Attributwert entsprechen.	Organisationen, bei denen "org Name=finance" ist	wobei <Org-Filter>
Die Organisation muss der benannten Organisation angehören.	Organisationen in "finance" und geringer	in <Org-Regel>
Die Organisation muss mit einem Attributwert übereinstimmen und der benannten Organisation angehören.	Organisationen, bei denen "org Name=finance" ist und die in "finance" und niedriger sind	wobei <Org-Filter> in <Org-filter> ist

Weitere Informationen:

Allgemeine Richtlinien zu Regeln (siehe Seite 30)

Allgemeine Richtlinien zu Regeln

Unabhängig davon, welche Art von Regel Sie erstellen, sollten Sie verstehen, wie sie in Identity Manager verarbeitet wird.

Auswerten von Operatoren

Beim Erstellen von Regeln für eine Rolle können Sie die Operatoren >=, <=, < und > einschließen. Diese Operatoren werden jedoch als Zeichenfolgen vom LDAP-Verzeichnis oder von der relationalen Datenbank ausgewertet. Die meisten Benutzerspeicher vergleichen Zeichenfolgen basierend auf dem Alphabet. Beim Vergleich von 500 mit 1100 kann der Benutzerspeicher deswegen bestimmen, dass 500 größer ist, weil 5 größer ist als 1.

Sie können die Art und Weise, wie Zeichenfolgen im Benutzerspeicher verglichen werden, möglicherweise ändern. Sehen Sie in der Dokumentation für den LDAP Directory Service oder die Software für relationale Datenbanken nach.

Nichtberücksichtigung der Groß- und Kleinschreibung von Regeln

Wenn Sie Admin- oder Zugriffsrollen erstellen, hängt es vom Benutzerspeicher ab, ob bei der Auswertung der erstellten Regeln die Groß- und Kleinschreibung berücksichtigt wird.

Nach dem Erstellen oder Ändern werden die Regeln intern jedoch ohne Berücksichtigung der Groß- und Kleinschreibung ausgewertet, bevor die Änderungen im Benutzerspeicher übernommen werden. Wenn eine Regel zum Beispiel die Bedingung "title=Manager" aufweist, stimmt die Regel mit einem Objekt im Benutzerspeicher unabhängig davon überein, ob der Wert des Titels "manager" oder "Manager" ist.

Hinzufügungs- und Entfernungsaktionen

Sie müssen sowohl eine Hinzufügungs- als auch eine Entfernungsaktion angeben, damit Identity Manager die Mitgliedschaft einer Rolle ordnungsgemäß verwaltet, wenn Administratoren die Rolle gewähren oder widerrufen.

- Bei der Hinzufügungsaktion muss der Benutzer die Kriterien in einer der Mitgliederregeln der Rolle erfüllen. Wenn zum Beispiel die Mitgliederregel für die Rolle "User Manager" festlegt, dass "User Manager" ein Wert des Attributs "Admin-Rollen" der Rollenmitglieder sein muss, muss "User Manager" mit der Hinzufügungsaktion zum Attribut "Admin-Rollen" hinzugefügt werden.
- Analog dazu sollte die Entfernungsaktion das Profil eines Benutzers so ändern, dass der Benutzer beim Widerrufen der Regel nicht mehr mit der Mitgliederregel übereinstimmt.

Jede Rolle kann zwei *Hinzufügungsaktionen* und zwei *Entfernungsaktionen* aufweisen.

Wenn Administratoren Rollenmitglieder hinzufügen und entfernen können, definieren Sie die Hinzufügungs- und Entfernungsaktionen. Andernfalls besitzt der Benutzer die Rolle, wenn er der Mitgliederregel entspricht und z. B. zur Gruppe "RoleAdmins" gehört. Beispiel:

- Rolle A kann von einem Administrator zugewiesen werden, sodass Hinzufügungs- oder Entfernungsaktionen definiert werden.
- Rolle B enthält eine Regel, dass alle Mitglieder der Gruppe "Finanzen" die Rolle besitzen. Diese Rolle kann nicht zugewiesen werden, und sie verfügt deshalb über keine Hinzufügungs- oder Entfernungsaktionen.

Wenn Sie Hinzufügungs- oder Entfernungsaktionen definieren, ziehen Sie in Betracht, das Attribut "Admin-Rollen" zu verwenden. Identity Manager kann mithilfe dieses Attributs eine Liste der Rollen des Benutzers speichern. Beispielsweise können Sie eine Hinzufügungsaktion konfigurieren, mit der "Employees" dem Attribut "Admin-Rollen" eines Benutzers hinzufügt wird, wenn dieser Benutzer der Rolle "Mitarbeiter" als Mitglied hinzugefügt wird. Wenn ein Administrator die Rolle "Mitarbeiter" einem Manager zuweist, der bereits die Rollen "Self Administrator" und "User Manager" besitzt, würde das Attribut "Admin-Rollen" des Managers die folgenden Werte enthalten: "Self Administrator", "User Manager", "Employee".

Damit das Attribut "Admin-Rollen" verwendet werden kann, muss das bekannte Attribut %ADMIN_ROLE_CONSTRAINT% einem Attribut mit mehreren Werten in den Benutzerprofilen zugeordnet werden. Weitere Informationen finden Sie im *CA Identity Manager-Konfigurationshandbuch*.

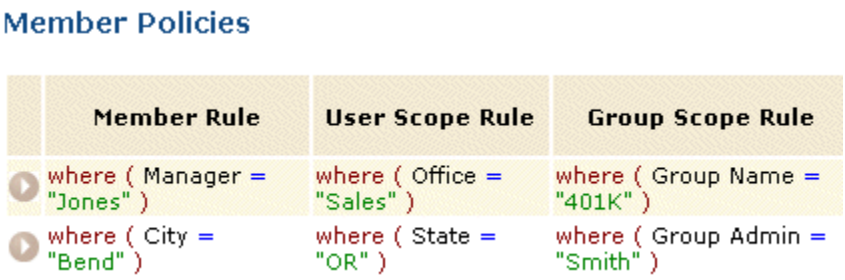
Wichtig! Vermeiden Sie es beim Definieren einer Hinzufügungsaktion, eine Regel einzurichten, die sich auf die Rolle bezieht, die Sie definieren. Definieren Sie zum Beispiel keine Hinzufügungsaktion, die angibt, dass ein Benutzer Mitglied der Rolle A ist, um ihn als Mitglied der Rolle A hinzuzufügen. Dadurch wird ein rekursiver Fehler generiert, der zu einem Neustart des Richtlinienservers führt.

Mitgliederrichtlinien

Eine *Mitgliederrichtlinie* gibt an, dass ein Benutzer, der der Mitgliederregel entspricht, über den in dieser Richtlinie definierten Bereich verfügt. Die folgende Abbildung zeigt eine Rolle mit zwei Mitgliederrichtlinien.

- Die erste Richtlinie gibt an, dass ein Rollenmitglied, dessen Manager Jones ist, die Rolle für Benutzer im "Sales Office" (Verkaufsbüro) verwenden und diese als Mitglieder der Gruppe "401K" verwalten kann.

- Die zweite Richtlinie gibt an, dass ein Rollenmitglied, das sich in der Stadt Bend befindet, die Rolle für Benutzer im Bundesstaat Oregon verwenden und diese als Mitglieder von Gruppen mit dem Gruppenadministrator Smith verwalten kann.

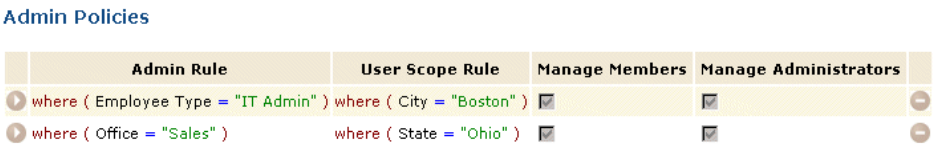

Member Policies
Member Rule
User Scope Rule
Group Scope Rule
where (Manager = "Jones")
where (Office = "Sales")
where (Group Name = "401K")
where (City = "Bend")
where (State = "OR")
where (Group Admin = "Smith")

Admin-Richtlinien

Eine *Admin-Richtlinie* gibt an, dass ein Benutzer, der der Admin-Regel entspricht, über den Benutzerbereich und die Administratorrechte verfügt, der/die in dieser Richtlinie definiert ist bzw. sind. Der Benutzerbereich legt fest, wo die Rolle verwendet wird. Die Administratorrechte bestimmen, ob der Rollenadministrator Mitglieder oder Administratoren der Rolle verwalten kann.

Die folgende Abbildung zeigt eine Rolle mit zwei Admin-Richtlinien, die folgendermaßen definiert sind:

- Gemäß der ersten Richtlinie kann ein IT-Admin unter den Benutzern in der Stadt Boston Rollenmitglieder und Administratoren hinzufügen und entfernen.
- Gemäß der zweiten Richtlinie kann ein Administrator in "Sales" (Verkauf) Mitglieder im Bundesstaat Ohio hinzufügen und entfernen.


Admin Policies
Admin Rule
User Scope Rule
Manage Members
Manage Administrators
where (Employee Type = "IT Admin")
where (City = "Boston")
where (Office = "Sales")
where (State = "Ohio")

Checkliste für die Rollenplanung

Verwenden Sie diese Checkliste mit Rollenmerkmalen, bevor Sie eine Rolle erstellen.

Rollenmerkmale	Details
Rollenprofil	Definieren Sie einen Namen und eine Beschreibung für die Rolle, und legen Sie den Status "Aktiviert" fest.
Aufgaben	Schließen Sie Admin- oder Zugriffsaufgaben ein.
Kontovorlagen	Schließen Sie Kontovorlagen ein, die Konten definieren, die in Endpunkten vorhanden sind (nur für Bereitstellungsrollen).
Mitgliederrichtlinien	Definieren Sie für jede Mitgliederrichtlinie Folgendes: ■ Mitgliederregeln - Wer die Rolle verwenden kann ■ Bereichsregeln - Welche Objekte ein Rollenmitglied verwalten kann ■ Hinzufügungsaktion - Was mit dem Profil eines Benutzers geschieht, der Mitglied wird ■ Entfernungsaktion - Was mit dem Profil eines Benutzers geschieht, der als Mitglied entfernt wird
Admin-Richtlinien	Definieren Sie für jede Admin-Richtlinie Folgendes: ■ Admin-Regeln - Wer die Benutzer als Mitglieder oder Administratoren verwalten kann ■ Bereichsregeln - Welche Benutzer der Administrator als Mitglieder oder Administratoren verwalten kann ■ Hinzufügungsaktion - Was mit dem Profil eines Benutzers geschieht, der Administrator wird ■ Entfernungsaktion - Was mit dem Profil eines Benutzers geschieht, der als Administrator entfernt wird
Eigentümerregeln	Legen Sie fest, wer die Rolle ändern kann.

Kapitel 2: Admin-Rollen

Dieses Kapitel enthält folgende Themen:

Admin-Rollen und Admin-Aufgaben (siehe Seite 35)
Erstellen von Admin-Rollen (siehe Seite 36)
Überprüfen von Admin-Rollen (siehe Seite 41)
Benutzern die Selbstzuweisung von Rollen gewähren (siehe Seite 42)

Admin-Rollen und Admin-Aufgaben

Basierend auf Ihren speziellen geschäftlichen Anforderungen erstellen Sie Rollen, die Aufgaben für das Verwalten von Objekten enthalten. So können Sie beispielsweise mehrere Rollen mit Aufgaben erstellen, mit denen Benutzer verwaltet werden, sowie weitere Rollen mit Aufgaben, mit denen die erstellten Rollen verwaltet werden.

Sie können auch separate Rollen mit den folgenden Aufgaben erstellen:

- Aufgaben für Administratoren zur Verwaltung von Benutzern
- Aufgaben zur Verwaltung der Administratoren
- Aufgaben zur Verwaltung der Admin-Rollen
- Aufgaben zur Verwaltung der Zugriffsrollen

Hinweis: Sie können auch die standardmäßigen Admin-Rollen verwenden, die in CA IdentityMinder enthalten sind. Diese Rollen weisen Aufgaben auf, die in Kategorien gruppiert sind, die jenen in der Liste oben ähneln.

Admin-Rollen und Identity Manager-Umgebungen

Nach der Anmeldung bei einer Identity Manager-Umgebung weist Ihr Benutzerkonto mindestens eine Admin-Rolle auf. Jede Admin-Rolle enthält Aufgaben (z. B. "Benutzer erstellen"), die Sie in dieser Identity Manager-Umgebung verwenden.

In der *zentralen* Identity Manager-Umgebung weist die Admin-Rolle *Helpdesk* beispielsweise Aufgaben zum Zurücksetzen von Kennwörtern auf. Laut der Mitgliederregel der Rolle muss es sich beim Benutzer um einen IT-Arbeitnehmer handeln. Wenn sich IT-Arbeitnehmer bei der *zentralen* Identity Manager-Umgebung anmelden, ist ihnen die Rolle *Helpdesk* zugewiesen, und sie können die Kennwörter der Benutzer in dieser Identity Manager-Umgebung zurücksetzen.

Admin-Rollen und die -Benutzerkonsole

Eine Identity Manager-Umgebung wird über die Benutzerkonsole angezeigt. Die Ihnen zugewiesenen Admin-Rollen bestimmen, welcher Inhalt in der Konsole angezeigt wird, wie in der folgenden Tabelle dargestellt:

Zugewiesene Rollen	Format der -Benutzerkonsole
System-Manager-Rolle	Die Kategorieliste aller Objekte und alle Standard-Admin-Aufgaben für die Verwaltung dieser Objekte
Rollen für die Verwaltung mehrerer Objekttypen	Die Kategorieliste mit je einem Element pro Objekttyp, den Sie verwalten können
Rollen für die Verwaltung eines Objekttyps, z. B. "Benutzer"	Die Aufgaben für dieses Objekt (z. B. "Benutzer ändern") *ohne* Kategorieliste
Genehmigungsrolle	Das Fenster "Arbeitsliste" Wird angezeigt, wenn der Administrator über Aufgaben verfügt, bei denen die Genehmigung noch aussteht (Benutzer, die sich selbst registrieren, benötigen z. B. eine Genehmigung)

Wenn Sie mehrere Objekte verwalten können, wird die Kategorieliste mit den Objekten angezeigt, die Sie ändern können. Diese Objekte (z. B. "Benutzer" und "Gruppen") werden oben im Fenster in Form von Registerkarten angezeigt. Wählen Sie eine Registerkarte aus, um die Aufgaben in den Ihnen zugewiesenen Rollen anzuzeigen.

Hinweis:: Falls Ihr Internetbrowser keine Cascading Style Sheets (CSS) unterstützt, wird von der -Benutzerkonsole ein anderes Format verwendet. Hinweise zum Steuern dieses Formats finden Sie im *Konfigurationshandbuch*.

Erstellen von Admin-Rollen

Sobald Sie die Anforderungen an die Rollen kennen, können Sie Admin-Rollen erstellen. Diese Anforderungen beziehen sich auf den jeweiligen Benutzer der Rolle, welche Objekte mit der Rolle verwaltet werden, und in welcher Umgebung die zu verwaltenden Objekte vorliegen.

Einführung in die Erstellung von Admin-Rollen

Admin-Rollen werden über die Benutzerkonsole erstellt.

So erstellen Sie Admin-Rollen:

1. Melden Sie sich bei einem CA IdentityMinder-Konto an, das eine Rolle mit Aufgaben zum Erstellen von Admin-Rollen aufweist.

   Dem ersten Benutzer einer Umgebung ist beispielsweise die System-Manager-Rolle zugewiesen, welche die Aufgabe "Admin-Rolle erstellen" aufweist.

2. Wählen Sie unter "Rollen und Aufgaben" die Option "Admin-Rollen" und dann "Admin-Rolle erstellen" aus.

3. Wählen Sie die Option zum Erstellen einer neuen Rolle oder einer Kopie einer Rolle aus.

   Die Registerkarte "Profil" wird an der Stelle angezeigt, an der Sie mit dem Definieren der Admin-Rolle beginnen.

4. Definieren Sie das Profil der Admin-Rolle.

Definieren des Profils der Admin-Rolle

Auf der Registerkarte "Profil" werden grundlegende Eigenschaften der Rolle definiert.

So definieren Sie das Profil:

1. Geben Sie einen Namen und eine Beschreibung ein, und legen Sie alle anderen benutzerdefinierten Attribute fest, die für die Rolle definiert sind.

   Hinweis: Sie können auf dem Register "Profil" benutzerdefinierte Attribute angeben, die weitere Informationen zu Admin-Rollen enthalten. Sie können diese zusätzlichen Informationen verwenden, um Rollensuchvorgänge in Umgebungen zu erleichtern, die eine große Anzahl von Rollen enthalten.

2. Wählen Sie die Option "Aktiviert" aus, wenn Sie die Rolle sofort nach der Erstellung für die Verwendung freigeben möchten.

3. Wählen Sie Admin-Aufgaben für die Rolle aus (siehe Seite 38).

Auswählen von Admin-Aufgaben für die Rolle

Auf der Registerkarte "Aufgaben" wählen Sie die Admin-Aufgaben aus, die in der Rolle enthalten sein sollen. Sie können Aufgaben aus anderen Kategorien hinzufügen oder Aufgaben kopieren, die in einer anderen Rolle verwendet werden.

So wählen Sie Admin-Aufgaben aus:

1. Wählen Sie die Kategorie im Feld "Nach Kategorie filtern" aus.

   Klicken Sie auf den Abwärtspfeil, um die Liste der verfügbaren Aufgabenkategorien anzuzeigen.

2. Wählen Sie die in die Rolle aufzunehmende Aufgabe im Feld "Aufgabe hinzufügen" aus.

   CA IdentityMinder fügt die Aufgabe der Aufgabenliste in der Rolle hinzu.

3. Führen Sie die Schritte 1 und 2 erneut aus, um weitere Aufgaben hinzuzufügen.

4. Sie können eine Aufgabe aus der Rolle löschen, indem Sie auf das Minussymbol ( ) für diese Aufgabe klicken.

5. Definieren Sie Mitgliederrichtlinien für eine Admin-Rolle (siehe Seite 39).

Definieren von Mitgliederrichtlinien für Admin-Rollen

Auf der Registerkarte "Mitglieder" werden Mitgliederrichtlinien erstellt, die bestimmen, welche Benutzer Rollenmitglieder werden können.

So definieren Sie Mitgliederrichtlinien:

1. Klicken Sie auf "Hinzufügen", um Mitgliederrichtlinien zu definieren. Mitgliederrichtlinien enthalten die folgenden Regeln:

   - Mitgliederrichtlinien, die die Anforderungen an Benutzer definieren, um zu einem Rollenmitglied zu werden.

     Hinweis: Die folgenden Operatoren behandeln Zahlen in Mitgliederregeln als Zeichen:

     - Kleiner als (<)
     - Kleiner oder gleich (<=)
     - Größer als (>)
     - Größer oder gleich (=>)

     "10" folgt beispielsweise auf "1", jedoch vor "2".

   - Bereichsregeln, die die primären und sekundären Objekte einschränken, die für Aufgaben in der Rolle verfügbar sind.

     Falls die Rolle beispielsweise eine Aufgabe enthält, die Benutzer durch das Zuweisen zu Gruppen ändert, schränkt die Benutzerbereichsregel die Benutzer ein (primäres Objekt), die gefunden werden können, und die Gruppenbereichsregel die Gruppen (sekundäres Objekt), die zugewiesen werden können.

   Hinweis: Stellen Sie sicher, dass Sie für mindestens eine Bereichsfrage eine Antwort eingeben. Bereichsregeln schränken die primären und sekundären Objekte ein, die für Aufgaben in der Rolle verfügbar sind. Falls die Rolle beispielsweise eine Aufgabe enthält, die Benutzer durch das Zuweisen zu Gruppen ändert, schränkt die Benutzerbereichsregel die Benutzer ein (primäres Objekt), die gefunden werden können, und die Gruppenbereichsregel die Gruppen (sekundäres Objekt), die zugewiesen werden können.

2. Überprüfen Sie, ob die Mitgliederrichtlinie auf der Registerkarte "Mitglieder" angezeigt wird.

   - Klicken Sie auf das Symbol mit dem Rechtspfeil auf der linken Seite, um eine Richtlinie zu bearbeiten.
   - Klicken Sie auf das Symbol mit dem Minuszeichen, um sie zu entfernen.

3. Aktivieren Sie auf der Registerkarte "Mitglieder" das Kontrollkästchen "Administratoren können Mitglieder dieser Rolle hinzufügen oder aus ihr entfernen", sofern Benutzer nicht ausschließlich dann Mitglieder werden sollen, wenn sie eine Mitgliederregel erfüllen.

   Nach dem Aktivieren dieser Funktion wird das Fenster erweitert.

4. Definieren Sie im erweiterten Bereich die Aktionen zum Hinzufügen und Entfernen für den Fall, dass Benutzer als Rollenmitglieder hinzugefügt bzw. entfernt werden.

   Wichtig! Vermeiden Sie beim Definieren einer Aktion zum Hinzufügen das Einrichten einer Regel, die auf die Regel verweist, die Sie erstellen. Definieren Sie beispielsweise keine Aktion zum Hinzufügen, die einen Benutzer zu einem Mitglied von Rolle A macht, wenn dieser bereits Mitglied der Rolle A ist. Dies kann zu Fehlern führen.

5. Definieren Sie Admin-Richtlinien für die Admin-Rollen (siehe Seite 40).

Definieren von Admin-Richtlinien für Admin-Rollen

Auf der Registerkarte "Administratoren" definieren Sie, wer Benutzer als Mitglieder und Administratoren dieser Rolle hinzufügen und entfernen darf.

So definieren Sie Admin-Richtlinien:

1. Aktivieren Sie das Kontrollkästchen "Administratoren können Administratoren dieser Rolle hinzufügen oder aus ihr entfernen.", wenn Sie die Option "Administratoren verwalten" verfügbar machen möchten.

   Nach dem Aktivieren dieser Funktion wird das Fenster erweitert.

2. Definieren Sie im erweiterten Bereich die Aktionen zum Hinzufügen und Entfernen für den Fall, dass ein Benutzer als Administrator der Rolle hinzugefügt bzw. entfernt wird.

3. Definieren Sie Admin-Richtlinien, die Admin- und Bereichsregeln und mindestens ein Administratorrecht ("Mitglieder verwalten" oder "Administratoren verwalten") enthalten.

   Hinweis: Sie können mehrere Admin-Richtlinien mit verschiedenen Regeln und unterschiedliche Berechtigungen für Administratoren hinzufügen, die die Regel einhalten.

4. Klicken Sie auf das Pfeilsymbol auf der linken Seite, um eine Richtlinie zu bearbeiten. Klicken Sie auf das Symbol mit dem Minuszeichen, um sie zu entfernen.

5. Definieren Sie Eigentümerregeln für eine Admin-Rolle (siehe Seite 41).

Definieren von Eigentümerregeln für Admin-Rollen

Auf der Registerkarte "Eigentümer" definieren Sie Regeln zu Benutzern, die Eigentümer der Rolle werden können. Hierbei handelt es sich um Benutzer, die Rollen ändern können.

So definieren Sie Eigentümerregeln:

1. Definieren Sie Eigentümerregeln, die bestimmen, welche Benutzer die Rolle ändern können.
2. Klicken Sie auf "Senden".

   Es wird eine Meldung mit der Information angezeigt, dass die Aufgabe gesendet wurde. Bevor Benutzer die Rolle verwenden können, kann es zu einer geringfügigen Verzögerung kommen.

Falls Sie beim Erstellen dieser Rolle die Option "Aktiviert" ausgewählt haben, steht die Rolle zur Verwendung zur Verfügung. Wenn Benutzer die Bedingungen in der Mitgliederregel erfüllen, können sich diese Benutzer nun bei der Identity Manager-Umgebung anmelden und die Aufgaben in der Rolle verwenden.

Überprüfen von Admin-Rollen

Um zu überprüfen, ob eine Rolle erstellt wurde, wählen Sie zunächst die Option "Admin-Rollen" aus und dann die Option "Admin-Rolle anzeigen" aus. Wählen Sie dann den Namen der Rolle aus.

Sie können auch die Option "System" und dann "Übermittelte Aufgaben anzeigen" auswählen, um anzuzeigen, ob die Aufgabe des Erstellens von Rollen abgeschlossen wurde.

Benutzern die Selbstzuweisung von Rollen gewähren

In einer Umgebung können Rollen vorhanden sein, die sich Benutzer selbst zuweisen können. Beispielsweise möchten Sie es unter Umständen zulassen, dass sich Benutzer für die Rolle des Delegierungs-Managers registrieren, damit sie Arbeitselemente eines Benutzers an einen anderen Benutzer delegieren können.

Um zu steuern, welche Rollen sich Benutzer selbst zuweisen können, konfigurieren Sie in der Aufgabe "Rollen-Selbstverwaltung" bestimmte Kriterien.

So gewähren Sie es Benutzern, sich Rollen selbst zuzuweisen:

1. Ändern Sie die Aufgabe "Rollen-Selbstverwaltung" wie folgt:
   a. Wählen Sie zunächst die Option "Rollen und Aufgaben" und dann die Option "Admin-Aufgabe ändern" aus, und suchen Sie dann nach der Aufgabe "Rollen-Selbstverwaltung".
   b. Wählen Sie die Registerkarte "Registerkarten" aus.

      CA IdentityMinder zeigt die Liste der Registerkarten an, die für diese Aufgabe verfügbar sind.
   c. Wählen Sie das Symbol mit dem Rechtspfeil neben der Registerkarte "Rollen-Selbstverwaltung" aus, um sie zu bearbeiten.
   d. Füllen Sie die folgenden Felder aus:

      Nur Admin-Rollen anzeigen, die die folgenden Regeln erfüllen

      Legt die Kriterien fest, mit denen CA IdentityMinder ermittelt, welche Rollen Benutzer sich selbst zuweisen dürfen.

      Zum Hinzufügen zusätzlicher Regeln klicken Sie auf das Plus-Symbol (+).

      Benutzer, der als Admin-Rollen-Administrator fungieren soll

      Legt den Administrator für Rollen fest, die Benutzer sich selbst zuweisen dürfen.

      Die Rollen, die Benutzer sich selbst zuweisen können, müssen den Benutzer enthalten, den Sie in diesem Feld als Administrator auswählen *und* den Kriterien entsprechen, die Sie im Feld "Nur Admin-Rollen anzeigen, die die folgenden Regeln erfüllen" angegeben haben.

      Listenfenster

      Legt die Spalten und das Format für die Liste der Rollen fest, die ein Benutzer auswählen kann, um sich selbst eine Rolle zuzuweisen.
   e. Klicken Sie auf "OK" und dann auf "Senden".
2. Fügen Sie die Aufgabe "Rollen-Selbstverwaltung" zu einer Regel hinzu, und weisen Sie diese Rolle Benutzern zu, die diese Option aufweisen sollen.

Kapitel 3: Admin-Aufgaben

Dieses Kapitel enthält folgende Themen:

Planen von Admin-Aufgaben (siehe Seite 43)
Verwendungsoptionen von Admin-Aufgaben (siehe Seite 48)
Standardmäßige Admin-Aufgaben (siehe Seite 49)
Erstellen von benutzerdefinierten Admin-Aufgaben (siehe Seite 50)
Definieren der Profile von Aufgaben (siehe Seite 51)
Definieren von Aufgabenbereichen (siehe Seite 56)
Auswählen von Registerkarten für Aufgaben (siehe Seite 67)
Anzeigen von Feldern in Aufgaben (siehe Seite 71)
Rollenverwendung anzeigen (siehe Seite 71)
Zuweisen von Workflow-Prozessen für Ereignisse (siehe Seite 72)
Verwalten eines Active Directory-Benutzerspeichers (siehe Seite 72)
Externe Aufgaben für Anwendungsfunktionen (siehe Seite 74)
Erweiterte Aufgabenkomponenten (siehe Seite 76)
Admin-Aufgaben und Ereignisse (siehe Seite 78)
Verarbeiten von Admin-Aufgaben (siehe Seite 80)
Bilder für Admin-Aufgaben (siehe Seite 84)

Planen von Admin-Aufgaben

Admin-Rollen bestehen aus Admin-Aufgaben, die genaue Funktionen für das Verwalten von Objekten darstellen. Beispielsweise kann ein Benutzerobjekt durch Verwendung dieser Admin-Aufgaben verwaltet werden:

- Benutzer erstellen
- Benutzer anzeigen
- Benutzer ändern
- Benutzerkennwort zurücksetzen

Jede Aufgabe wird so erstellt oder geändert, dass sie den Anforderungen genau entspricht. Die entsprechenden Admin-Aufgaben werden dann zu Admin-Rollen zusammengefasst und Administratoren zugewiesen. Durch diese Rollen haben die Administratoren genau die Berechtigungen, die sie zum Verwalten von Objekten benötigen.

Legen Sie zum Planen der Erstellung von Admin-Aufgaben fest, welche Objekte verwaltet werden müssen (Benutzer, Gruppe, Organisation, Rolle oder Aufgabe) und welche Administratoren die Aufgaben verwenden werden. Beispiel:

- Zur Verwaltung von Benutzern benötigen Helpdesk-Administratoren Aufgaben, die Benutzerattribute verwalten (z. B. Benutzer-ID oder Titel).
- Zur Verwaltung des Zugriffs von Benutzern auf Anwendungen benötigen andere Administratoren Aufgaben, die Benutzer zu Mitgliedern von Zugriffsrollen machen.
- Zur Verwaltung der Rollen, die von Helpdesk-Administratoren verwendet werden, benötigen Administratoren auf höherer Ebene Aufgaben, die Admin-Rollen verwalten.

Für einen Objekttyp (z. B. Benutzer) können Sie Aufgaben erstellen, so dass verschiedene Administratoren unterschiedliche Attribute verwalten. In der folgenden Abbildung ist beispielsweise ein Benutzer dargestellt, der von zwei Administratoren verwaltet wird.

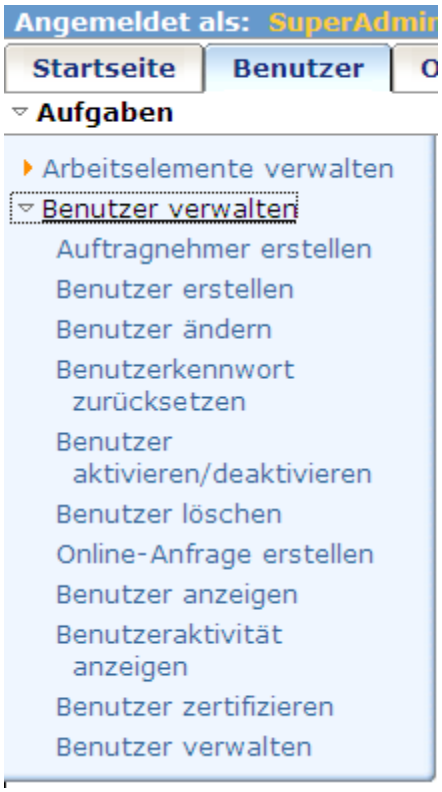
- Admin 1 weist die Aufgabe "Benutzerkennwort zurücksetzen" auf. Dieser Administrator kann die Benutzer-ID und den Namen des Arbeitnehmers anzeigen bzw. dessen Kennwort zurücksetzen.
- Admin 2 weist die Aufgabe "Benutzer ändern" auf. Dieser Administrator kann die Benutzer-ID und den Namen des Arbeitnehmers anzeigen bzw. dessen Titel und Urlaubstage ändern.

Beispiel einer Admin-Aufgabe

Beim Erstellen einer Admin-Aufgabe werden der Inhalt und das Layout von Fenstern in der Aufgabe definiert. Hierzu zählen:

- Der Name der Aufgabe
- Die Kategorie, in der die Aufgabe angezeigt wird
- Die Registerkarten und Felder, die in der Aufgabe verwendet werden sollen, und die Feldanzeigeeigenschaften
- Die Felder, die Administratoren in einer Suchabfrage verwenden können, und die Felder, die in den Suchergebnissen angezeigt werden

Betrachten Sie sich zum Verständnis der Elemente einer Aufgabe die Aufgabe "Benutzer ändern". In diesem Fall stellt "Benutzer" die Kategorie, "Benutzer verwalten" eine Unterkategorie und "Benutzer ändern" die Aufgabe dar. Die Kategorie und der Aufgabenname werden beim Erstellen der Aufgabe erstellt.



Wenn Sie "Benutzer ändern" auswählen wird ein Suchfenster eingeblendet. Über ein *Suchfenster* stehen Optionen für die Suche nach Objekten zur Verfügung, die Sie anzeigen oder ändern möchten. Jede Option fungiert als *Filter*, der die Objekte einschränkt, die bei der Suche gefunden werden.

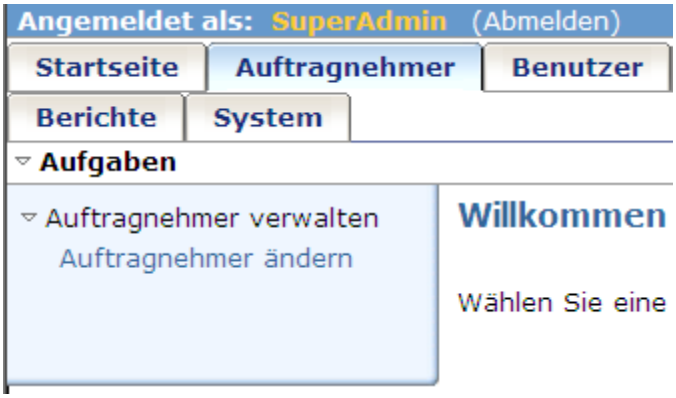
Nach dem Ausfüllen der Felder im Suchfenster wird ein Fenster mit Registerkarten angezeigt. In der folgenden Abbildung sind beispielsweise die Registerkarten für die Aufgabe "Benutzer ändern" dargestellt. Als Erstes wird die Registerkarte "Profil" angezeigt, auf der die Benutzerattribute angezeigt werden. Die anderen Registerkarten zeigen die Rollen- und Gruppenberechtigungen des Benutzers an.

Bei der Aufgabe, die Sie erstellen, bestimmen Sie, welche Registerkarten enthalten sein sollen sowie deren Reihenfolge und Inhalt.

Wenn Sie beispielsweise die Aufgabe "Benutzer ändern" als Vorlage verwenden, können Sie die Aufgabe "Auftragnehmer ändern" erstellen, die Änderungen in folgenden Bereichen aufweist:

- Die Felder auf der Registerkarte "Profil"
- Die Registerkarten, die in der Aufgabe enthalten sein sollen, und deren Inhalt
- Die Kategorie, unter der die Aufgabe angezeigt wird

  Sie können diese Aufgabe unter einer neuen Kategorie "Auftragnehmer" erstellen.



Die Aufgabe "Auftragnehmer ändern" enthält einige der Felder der Registerkarte "Profil" aus der Aufgabe "Benutzer ändern" sowie weitere Felder, zum Beispiel das Startdatum des Auftrags und das Unternehmen des Auftragnehmers. Administratoren können nach einem Auftragnehmer suchen, indem sie nach dem Namen des Auftragnehmers, dem Unternehmen oder dem Startdatum suchen.

Die neue Aufgabe enthält darüber hinaus die Registerkarte "Auftragnehmerrollen", auf der Rollen für Auftragnehmer hinzugefügt werden.

Verwendungsoptionen von Admin-Aufgaben

Admin-Aufgaben können in Identity Manager auf zwei Arten verwendet werden:

- **Auswählen der Aufgabe**

  Sie wählen eine Kategorie und eine Aufgabe aus und suchen dann nach dem Objekt, auf das sich die Aufgabe bezieht.

  Um beispielsweise ein Benutzerprofil zu ändern, wählen Sie die Kategorie "Benutzer" und dann die Aufgabe "Benutzer ändern" aus. Daraufhin suchen Sie dann nach dem Benutzer, der geändert werden soll.

- **Auswählen des Objekts**

  Sie verwenden Verwaltungsausgaben wie "Benutzer verwalten" oder "Gruppen verwalten", um nach einem Objekt zu suchen. Nach Auswählen des Objekts können Sie eine Liste mit Aufgaben anzeigen, die Sie zum Verwalten dieses Projekts verwenden können. Diese Methode bezeichnet man als *Objekt-Aufgaben-Navigation.*

  Wenn Sie beispielsweise einen Benutzer mit Hilfe dieser Methode ändern möchten, wählen Sie zunächst die Kategorie "Benutzer" und dann die Aufgabe "Benutzer verwalten" aus. Sie wählen den Benutzer aus, den Sie verwalten möchten. In den Suchergebnissen klicken Sie auf ein Symbol, um eine Liste mit Aufgaben anzuzeigen, die Sie zum Verwalten des ausgewählten Benutzers verwenden können. In dieser Liste können Sie die Aufgabe "Benutzer ändern" bzw. eine beliebige andere passende Aufgabe auswählen.

  Sie können Aufgabenlisten auch in anderen als den Verwaltungsaufgaben konfigurieren. Sie können eine Aufgabenliste beispielsweise zur Registerkarte "Mitgliedschaft" hinzufügen. In diesem Fall ist für jedes Mitglied eine Aufgabenliste verfügbar, das auf der Registerkarte "Mitgliedschaft" angezeigt wird.

  Hinweis: In der Aufgabenliste für ein Objekt werden nur Aufgaben angezeigt, die der aktuelle Administrator verwenden kann.

Standardmäßige Admin-Aufgaben

CA IdentityMinder enthält eine Reihe von Standard-Admin-Aufgaben und -Rollen. Dazu wird eine Rollendefinitionsdatei in die Managementkonsole von CA IdentityMinder importiert. Wenn Sie in der Managementkonsole eine Umgebung erstellen und wählen, die Standardrollen zu erstellen, importiert CA IdentityMinder automatisch eine Rollendefinitionsdatei.

Hinweis: Für einige Funktionen (z. B. die Kontenverwaltung für bestimmte Endpunkttypen) ist es erforderlich, zusätzliche Rollendefinitionsdateien zu importieren, um die notwendigen Rollen und Aufgaben zu erstellen.

In den meisten Fällen genügen die installierten Standardaufgaben. Sie müssen jedoch gegebenenfalls die Registerkarte "Profil" in den Standardbenutzeraufgaben wie "Benutzer erstellen", "Benutzer ändern" und "Benutzer anzeigen" ändern. Die Registerkarte "Profil" enthält alle Felder, die in der Verzeichniskonfigurationsdatei für das Benutzerobjekt definiert sind. Möglicherweise möchten Sie die Feldanzeigeeigenschaften ändern oder die Anzahl der Felder verringern, die auf der Registerkarte angezeigt wird.

Hinweis: Es wird empfohlen, nicht die Standardaufgabe selbst zu ändern, sondern eine Kopie der Standardaufgabe zu erstellen und diese zu ändern.

Erstellen von benutzerdefinierten Admin-Aufgaben

Bei einer *Admin-Aufgabe* handelt es sich um eine Verwaltungsfunktion, die Benutzer in Identity Manager ausführen können. Beispiele für Admin-Aufgaben sind "Benutzer erstellen", "Gruppe ändern" und "Rollenmitgliedschaft anzeigen".

CA IdentityMinder enthält Standard-Admin-Aufgaben, die Sie ändern und an die Bedürfnisse Ihrer Organisation anpassen können.

Beim Erstellen einer benutzerdefinierten Admin-Aufgabe werden folgende Schritte ausgeführt:

Hinweis: Der Abschnitt Active Directory-Voraussetzungen (siehe Seite 72) enthält zusätzliche Hinweise, wenn Identity Manager einen Active Directory-Benutzerspeicher verwaltet.

1. Wählen Sie in der Identity Manager-Benutzerkonsole folgende Befehle aus: "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe erstellen".

   Identity Manager prüft, ob Sie eine neue Aufgabe oder eine Aufgabe erstellen möchten, die auf einer vorhandenen Aufgabe basiert.

   Wählen Sie beispielsweise die Aufgabe "Benutzer ändern" als Grundlage für die neue Aufgabe aus.

2. Wählen Sie "Kopie einer Admin-Aufgabe erstellen" und suchen Sie nach der zu kopierenden Aufgabe.

   Hinweis: Es wird empfohlen, die Kopie einer Standardaufgabe und nicht die Standardaufgabe selbst zu ändern.

3. Nachdem Sie auf "OK" geklickt haben, wird ein Fenster mit den folgenden sechs Registerkarten angezeigt:

Registerkarte	Zweck	Thema mit weiteren Informationen
Profil	Definieren des Profils der Aufgabe, die erstellt wird	Definieren der Profile von Aufgaben (siehe Seite 51)
Suchen	Einschränken des Objektbereichs, der von der Aufgabe verwaltet wird	Definieren von Aufgabenbereichen (siehe Seite 56)
Registerkarten	Auswählen und Gestalten der Registerkarten für die Aufgabe	Auswählen von Registerkarten für Aufgaben (siehe Seite 67)
Felder	Anzeigen aller Felder, die bei allen Registerkarten verwendet werden	Anzeigen von Feldern in Aufgaben (siehe Seite 71)
Ereignisse	Auswählen eines Workflow-Prozesses für jedes Ereignis, falls in der Identity Manager-Umgebung und der Aufgabe Workflows verwendet werden	Zuweisen von Workflow-Prozessen für Ereignisse (siehe Seite 72)

Registerkarte	Zweck	Thema mit weiteren Informationen
Rollengebrauch	Zeigt die Rollen an, die die von Ihnen angezeigte oder geänderte Aufgabe enthalten.	Rollenverwendung anzeigen (siehe Seite 71)

Definieren der Profile von Aufgaben

Die Registerkarte "Profil" enthält allgemeine Einstellungen für die Aufgabe.

So definieren Sie das Profil der Aufgabe:

1. Wählen Sie den Objekttyp für die Aufgabe (das so genannte primäre Objekt) und die Aktion aus, die ausgeführt werden soll.
2. Füllen Sie alle erforderlichen Felder aus, und wählen Sie die entsprechenden Kontrollkästchen aus, die für die Aufgabe erforderlich sind.

   Hinweis: Wenn Sie eine Aufgabe erstellen, die ähnliche Profileinstellungen wie eine vorhandene Aufgabe aufweist, klicken Sie auf "Profil aus einer anderen Aufgabe kopieren". Mit dieser Option werden die Profileinstellungen der Aufgabe, die Sie erstellen, mit den Profileinstellungen einer vorhandenen Aufgabe gefüllt, die Sie auswählen. Fügen Sie anschließend einen Namen und eine Beschreibung für die neue Aufgabe hinzu.
3. (Optional) Weisen Sie der Aufgabe einen Business Logic Task-Handler zu.
4. Fahren Sie nach dem Vervollständigen dieser Registerkarte mit dem Schritt Definieren von Aufgabenbereichen (siehe Seite 56) fort.

Registerkarte "Profil" beim Erstellen einer Admin-Aufgabe

Auf der Registerkarte "Profil" von Admin-Aufgaben können Sie allgemeine Einstellungen für Admin-Aufgaben definieren.

Diese Registerkarte enthält die folgenden Felder:

- **Name**

  Gibt den Namen der Aufgabe an.

- **Tag**

  Gibt den eindeutigen Bezeichner für die Aufgabe an. Dieser wird in URLs, Webservices bzw. Eigenschaftendateien verwendet. Das Tag darf Buchstaben (a-z, A-Z), Ziffern (0-9) oder Unterstriche enthalten und muss mit einem Zeichen oder Unterstrich beginnen.

- **Beschreibung**

  Gibt einen optionalen Hinweis zum Zweck der Aufgabe an.

- **Aufgabenreihenfolge**

  Gibt die Anzeigereihenfolge für Aufgaben an. Falls keine Reihenfolge angegeben ist, werden die Aufgaben in alphabetischer Reihenfolge angezeigt.

- **Kategorie**

  Gibt eine Kategorie für die Aufgabe an. Kategorien werden oben im Fenster als Registerkarten angezeigt.

- **Kategorie-Reihenfolge**

  Gibt die Reihenfolge an, in der die Kategorieregisterkarte angezeigt wird. Wenn Sie die Kategorie-Reihenfolge beispielsweise mit 3 festlegen, wird die angegebene Kategorie als dritte Registerkarte angezeigt.

- **Kategorie 2**

  Gibt die Kategorie der zweiten Ebene an, die als Link unter der Liste der Kategorieregisterkarten angezeigt wird. Die Kategorie der zweiten Ebene wird nur angezeigt, wenn die Registerkarte der Kategorie der ersten Ebene ausgewählt ist. Wenn Sie beispielsweise eine Aufgabe mit der Kategorie der ersten Ebene "Arbeitnehmer" und der Kategorie der zweiten Ebene "Arbeitnehmerverwaltung" erstellt haben, wird die Kategorie "Arbeitnehmerverwaltung" erst angezeigt, wenn Sie die Registerkarte "Arbeitnehmer" ausgewählt haben.

- **Kategorie 2-Reihenfolge**

  Gibt die Reihenfolge an, in der die Kategorien der zweiten Ebene angezeigt werden, wenn in einer primären Kategorie mehrere Kategorien der zweiten Ebene vorhanden sind.

- **Kategorie 3**

  Gibt die Kategorie der dritten Ebene an, die im linken Navigationsfenster angezeigt wird. Aufgaben sind unter den Kategorien der dritten Ebene aufgeführt. In einer Standardumgebung wird einem Benutzer mit der Rolle des System-Managers bzw. Benutzer-Managers beispielsweise die Kategorie "Benutzer verwalten" angezeigt, wenn er die Registerkarte "Benutzer" auswählt.

- **Kategorie 3-Reihenfolge**

  Gibt die Reihenfolge an, in der die Kategorien der dritten Ebene angezeigt werden.

- **Primäres Objekt**

  Gibt das Objekt an, auf der die Aufgabe ausgeführt wird.

- **Aktion**

  Gibt den für das Objekt auszuführenden Vorgang an.

- **Benutzersynchronisierung**

  Gibt an, ob die Aufgabe Benutzer mit Identitätsrichtlinien synchronisiert. Sie können aus den folgenden Optionen wählen:

  - **Deaktiviert** (Standard)

    Gibt an, dass diese Aufgabe keine Benutzersynchronisierung auslöst.

  - **Bei Abschluss der Aufgabe**

    Gibt an, dass CA IdentityMinder den Prozess der Benutzersynchronisierung startet, nachdem alle Ereignisse in einer Aufgabe abgeschlossen sind. Diese Einstellung ist die Standardsynchronisierungsoption für die Aufgaben "Benutzer erstellen", "Benutzer ändern" und "Benutzer löschen". Die Standardeinstellung für alle anderen Aufgaben lautet "Deaktiviert".

    Hinweis: Beim Aktivieren der Option "Bei Abschluss der Aufgabe" für eine Aufgabe, die mehrere Ereignisse einschließt, synchronisiert CA IdentityMinder die Benutzer erst dann, wenn alle Ereignisse in der Aufgabe abgeschlossen sind. Falls für eines oder mehrere Ereignisse die Genehmigung des Workflows erforderlich ist, kann dieser Prozess mehrere Tage dauern. Um zu vermeiden, dass CA IdentityMinder mit der Anwendung der Identitätsrichtlinien wartet, bis alle Ereignisse abgeschlossen sind, wählen Sie die Option "Bei jedem Ereignis" aus.

  - **Bei jedem Ereignis**

    Gibt an, dass CA IdentityMinder den Prozess der Benutzersynchronisierung (siehe Seite 488) startet, wenn jedes Ereignis in einer Aufgabe abgeschlossen ist.

    Bei Aufgaben mit einem primären und sekundären Ereignis für den gleichen Benutzer kann das Festlegen der Benutzersynchronisierung mit "Bei jedem Ereignis" dazu führen, dass bei einem Benutzer mehr Identitätsrichtlinien angewendet werden als bei Auswahl der Option "Bei Abschluss der Aufgabe".

- **Kontosynchronisierung**

  Synchronisiert bei Aktivierung des Bereitstellungsservers Konten, die auf dem Bereitstellungsserver vorhanden sind.

  - **Deaktiviert** (Standard)

    Gibt an, dass diese Aufgabe keine Kontosynchronisierung auslöst.

  - **Bei Abschluss der Aufgabe**

    Gibt an, dass CA IdentityMinder den Prozess der Kontosynchronisierung startet, nachdem alle Ereignisse in einer Aufgabe abgeschlossen sind.

- **Bei jedem Ereignis**

  Gibt an, dass CA IdentityMinder den Prozess der Kontosynchronisierung startet, wenn jedes Ereignis in einer Aufgabe abgeschlossen ist.

  Hinweis: Mit Auswahl der Option "Bei Abschluss der Aufgabe" werden die besten Ergebnisse erzielt. Beim Aktivieren der Option "Bei Abschluss der Aufgabe" für eine Aufgabe, die mehrere Ereignisse einschließt, synchronisiert CA IdentityMinder die Benutzer allerdings erst dann, wenn alle Ereignisse in der Aufgabe abgeschlossen sind. Falls für eines oder mehrere Ereignisse die Genehmigung des Workflows erforderlich ist, kann dieser Prozess mehrere Tage dauern. Um zu vermeiden, dass CA IdentityMinder mit der Synchronisierung von Konten wartet, bis alle Ereignisse abgeschlossen sind, aktivieren Sie die Option "Bei jedem Ereignis".

- **In Menüs ausblenden**

  Verhindert, dass die Aufgabe in Menüs angezeigt wird. Aktivieren Sie dieses Steuerelement, wenn die Aufgabe nur von URLs oder anderen Aufgaben aufgerufen wird.

- **Öffentliche Aufgabe**

  Macht die Aufgabe für Benutzer verfügbar, die nicht bei CA IdentityMinder angemeldet sind. Zu den standardmäßigen öffentlichen Aufgaben zählen "Kennwort vergessen" und die Selbstregistrierung.

- **Überprüfung aktivieren**

  Zeichnet Informationen zur Aufgabe in einer Überprüfungsdatenbank auf. Überprüfungsinformationen können zum Generieren von Berichten verwendet werden. Detaillierte Informationen hierzu finden Sie im *Konfigurationshandbuch*.

- **Workflow aktivieren**

  Aktiviert bei installierter Workflow-Engine die mit einer Aufgabe verknüpften CA IdentityMinder-Ereignisse zum Auslösen von Workflow-Prozessen. Die Ereignisse, die mit der Aufgabe "Gruppe löschen" verknüpft sind, können beispielsweise einen Workflow-Prozess auslösen, der einen Genehmigungsschritt umfasst.

- **Webservices aktivieren**

  Markiert die Aufgabe als solche, für die über die Management-Konsole eine Web Services Description Language-Ausgabe (WSDL-Ausgabe) generiert werden kann. Aktivieren Sie dieses Steuerelement, wenn Sie die Remote-Aufgabenübermittlung verwenden möchten. Weitere Informationen finden Sie im *Programmierhandbuch für Java.*

- **Workflow-Prozess**

  Ermöglicht Konfigurationen für Workflows auf Aufgabenebene. Klicken Sie auf das Stift-Symbol, um einen richtlinienbasierten oder nicht richtlinienbasierten Workflow zu konfigurieren.

- **Aufgabenpriorität**

  Bestimmt die Reihenfolge, in der CA IdentityMinder Aufgaben ausführt. Aufgaben mit hoher Priorität werden vor Aufgaben mit mittlerer und niedriger Priorität ausgeführt. Die Standardpriorität einer Aufgabe lautet "Mittel".

  Hinweis: Sie können die Aufgabe "Gesendete Aufgaben anzeigen" verwenden, um nach Aufgaben mit einer bestimmten Priorität zu suchen und dann deren Status anzuzeigen.

- **Business Logic Task-Handler**

  Weist der Aufgabe einen Business Logic Task-Handler (siehe Seite 77) zu.

- **Schaltflächen für Workflow-Aktionen**

  Hiermit werden benutzerdefinierte Aktionsschaltflächen zu Workflow-Genehmigungsaufgaben hinzugefügt.

- **Profil aus einer anderen Aufgabe kopieren**

  Kopiert Daten von der Registerkarte "Profil" einer anderen Aufgabe.

  Sie können beispielsweise die Einstellungen der Registerkarte "Profil" aus der Aufgabe "Benutzer ändern" kopieren und dann einen Namen und eine Beschreibung hinzufügen.

Aufgaben-Konfigurationseigenschaften

Aufgaben-Konfigurationseigenschaften steuern Anzeigeeigenschaften und bestimmte Verhaltensweisen für die Aufgabe.

Pfad zum Aufgabensymbol

Angabe der URL für eine Grafik, die als Symbol für diese Aufgabe in Aufgabenlisten benutzt wird.

Vorschau des Aufgabensymbols

Zeigt das Symbol für die Aufgabe an, wie es in Aufgabenlisten angezeigt wird.

Aufgaben-Navigation unterdrücken

Bei Aktivierung wird die Navigation der obersten Ebene und die Aufgabenliste ausgeblendet, sobald ein Benutzer eine Aufgabe auswählt. Dies hält Benutzer davon ab, von der aktuellen Aufgabe weg zu navigieren, bis sie erforderliche Aktionen abgeschlossen haben oder die Aufgabe abbrechen.

Zielfenster

Wenn Sie einen Wert in diesem Feld angeben, öffnet CA IdentityMinder diese Aufgabe in einem neuen Browserfenster. Verwenden Sie dieses Feld, um ein neues Browserfenster für eine externe Aufgabe zu öffnen, die Benutzer an eine andere Website umleitet.

Sie können einen beliebigen Namen für das Fenster angeben.

Hinweis: Verwenden Sie dieses Feld nicht, um Admin-Aufgaben in einem separaten Browserfenster zu öffnen. CA IdentityMinder unterstützt nicht mehrere Browserfenster für eine einzelne CA IdentityMinder-Benutzersitzung.

Definieren von Aufgabenbereichen

Auf der Registerkarte "Suchen" wird der Aufgabenbereich definiert. Hiermit werden die Objekte eingeschränkt, die der Aufgabe zur Verfügung stehen. Wenn es sich bei dem Objekt einer Aufgabe beispielsweise um Benutzer handelt, können Sie den Bereich als Benutzer definieren, die Auftragnehmer sind.

Hinweis: Wenn die Aufgabe kein primäres Objekt aufweist bzw. wenn die Aktion "Selbständernd", "Selbstansicht" oder "Bestätigen" lautet, steht die Registerkarte "Suchen" nicht zur Verfügung.

Auf der Registerkarte "Suchen" werden folgende Einstellungen konfiguriert:

Suchfenster

Durch das Suchfenster wird der Bereich der Aufgabe basierend auf Filtern eingeschränkt. Klicken Sie auf "Durchsuchen", um die verfügbaren Suchfensteroptionen anzuzeigen:

Hinweis: Unter Umständen empfiehlt sich die Erstellung eines eigenen Suchfensters (siehe Seite 58). Wenn Sie eine geänderte Version eines bestehenden Suchfensters erstellen möchten, wählen Sie das entsprechende Suchfenster aus, und klicken Sie dann auf "Kopieren". Sie können das Suchfenster ändern, ohne die ursprüngliche Suchfensterdefinition zu verändern. Klicken Sie zur Erstellung eines Suchfensters auf "Neu".

Suchoptionen

Die Suchoptionen werden nur angezeigt, wenn es sich bei dem Objekt um eine Rolle oder Gruppe handelt.

- Mit der ersten Option wird die Suche basierend auf Feldern eingeschränkt, die im Suchfenster definiert werden. Gemäß diesen Einschränkungen werden bei der Suche sämtliche Gruppen bzw. Rollen im Bereich des Administrators ausfindig gemacht.
- Andere Optionen schränken die Suche wie angegebenen ein.

Beachten Sie Folgendes:

- Standardmäßig wird in den gruppenbezogenen Suchfenstern das Filtern unterstützt. Administratoren können folglich Kriterien angeben, um den Bereich von Gruppensuchen einzuschränken. Wenn Sie die Filterfunktion entfernen möchten, erstellen Sie ein Suchfenster, das keine Felder enthält, die in eine Suchabfrage aufgenommen werden könnten.
- Wenn es sich bei dem Objekt um eine Rolle handelt, wird auf der Registerkarte "Suchen" *Filtern wird nicht unterstützt* angezeigt, was besagt, dass die Aufgabe die Rollen anzeigt, die die Kriterien der von Ihnen ausgewählten Option erfüllen. Suchfelder, die im Suchfenster konfiguriert wurden, werden ignoriert.

Geänderte Objekte müssen im Bereich des Administrators bleiben

Ist dieses Kontrollkästchen aktiviert, gibt CA IdentityMinder eine Fehlermeldung aus, wenn an der Aufgabe vorgenommene Änderungen dazu führen, dass sich das primäre Objekt nicht mehr im Bereich des Administrators befindet. So kann beispielsweise ein Administrator mit Hilfe von "Benutzer ändern" das Attribut "Arbeitnehmertyp" eines Benutzers in "Manager" ändern. Diese Änderung führt u. U. dazu, dass sich der Benutzer nicht mehr im Bereich des Administrators befindet.

Suchfensterkonfiguration

Die Konfiguration eines Suchfensters dient dazu, den Bereich der Aufgabe einzuschränken und die Felder zu steuern, die die Benutzer zur Suche heranziehen können. Suchfenster beziehen sich auf zwei Arten von Objekten:

- Ein *primäres Objekt*–Das Objekt, das von der Aufgabe geändert bzw. angezeigt werden soll.
- Ein *sekundäres Objekt*–Das Objekt, das mit dem primären Objekt verwandt ist.

  Wenn Sie beispielsweise eine Aufgabe vom Typ "Benutzer erstellen" um eine Registerkarte vom Typ "Gruppe" ergänzen, ist der Benutzer das primäre Objekt und die Gruppe das sekundäre Objekt. Die Registerkarte "Gruppe" muss über ein Suchfenster für Gruppen verfügen.

  Hinweis: Nachdem Sie ein Suchfenster konfiguriert haben, können Sie es in jeder beliebigen Aufgabe zur Suche nach einem primären bzw. sekundären Objekt nutzen.

Suchfilter

Mit Suchfiltern wird eingeschränkt, welche Objekte beim Suchvorgang zurückgegeben werden. Handelt es sich bei dem Objekt beispielsweise um Benutzer, können Sie die Suche so einschränken, dass nur Auftragnehmer gefunden werden. Sie können einen Filter zur Suche nach Benutzern konfigurieren, deren Arbeitnehmertyp Auftragnehmer lautet.

Sie können für Suchvorgänge die folgenden Felder konfigurieren:

Nur Objekte anzeigen, die die folgenden Regeln erfüllen

Definiert zusätzliche Kriterien, die zur Eingrenzung der Suche mit dem benutzerdefinierten Filter kombiniert werden sollen.

Beachten Sie Folgendes, wenn Sie dieses Feld verwenden**:**

- Aufgrund von Einschränkungen bei Suchvorgängen, die sich auf Bereitstellungsrollen beziehen, werden Filterfelder, die durch den Benutzer eingegeben wurden, von Kriterien überschrieben, die denselben Namen aufweisen.
- Attribute, die bei der Konfiguration dieses Feldes verwendet werden, sollten im Suchfenster nicht als verfügbare Suchfelder angezeigt werden.

  Beispiel: Wenn Sie das Suchfenster so konfigurieren, dass nur Rollen angezeigt werden, bei denen das Attribut "Aktiviert" auf "JA" eingestellt ist, dann entfernen Sie das Attribut "Aktiviert" aus der Attributliste, über die der Benutzer Suchkriterien festlegen kann.

  Andernfalls werden die vom Benutzer eingegebenen Kriterien ignoriert.

Standard-Suchfilter

Definiert einen Filter, der standardmäßig angezeigt wird, wenn ein Administrator das Suchfenster nutzt. Wenn Sie beispielsweise ein Suchfenster für die Aufgabe "Auftragnehmer ändern" konfigurieren und wissen, dass die Administratoren normalerweise anhand des Namens des beauftragten Unternehmens nach Auftragnehmern suchen, können Sie den Standardfilter auf "Beauftragtes Unternehmen = *" einstellen. Administratoren können den Standardfilter außer Kraft setzen, indem sie abweichende Suchkriterien angeben. Die Definition eines Standardfilters führt zur Leistungsoptimierung, da die Anzahl der zurückgegebenen Ergebnisse eingeschränkt wird, wenn ein Administrator vor dem Suchvorgang keinen Filter angibt.

Bei Verwendung mit Mehrfachauswahl-Aufgaben alle Suchergebnisse automatisch markieren.

Gibt an, dass sämtliche Suchergebnisse standardmäßig ausgewählt sind. Wenn Sie dieses Kontrollkästchen aktivieren, wird neben dem Namen sämtlicher Objekte in der Suchergebnisliste ein Kontrollkästchen angezeigt.

Suche automatisch ausführen

Gibt an, dass zusätzlich zu den Suchergebnissen ein Feld mit Suchkriterien angezeigt wird.

Das Subjekt der Aufgabe wird automatisch festgelegt, wenn nur ein Suchergebnis vorliegt

Legt das primäre Objekt der Aufgabe automatisch fest, wenn nur ein einziges Objekt dem Suchfilter entspricht.

Angenommen, diese Option ist für ein Benutzersuchfenster aktiviert, das mit der Aufgabe "Benutzer ändern" verknüpft ist. Ruft ein Administrator die Aufgabe "Benutzer ändern" auf und gibt einen Suchfilter ein, bei dem nur ein Benutzer zurückgegeben wird, öffnet CA IdentityMinder die Aufgabe "Benutzer ändern" für diesen Benutzer. Der Administrator muss also den Benutzer nicht auswählen, um die Aufgabe "Benutzer ändern" zu öffnen.

Hinweis: Damit diese Einstellung gültig ist, müssen Sie auch "Suche automatisch ausführen" aktivieren.

Suchfilter speichern

Legt fest, dass der Suchfilter für die Aufgabe für den Benutzer in der aktuellen Sitzung gespeichert wird. Wenn ein Benutzer das nächste Mal einen Suchvorgang in der Aufgabe durchführt, wird der gespeicherte Suchfilter angezeigt.

Hinweis: CA IdentityMinder speichert den Suchfilter für die Dauer der Benutzersitzung. Wenn sich der Benutzer abmeldet, wird der Suchfilter gelöscht.

Innerhalb der Organisation suchen

Zeigt im Suchfenster einen Organisationsfilter an. Ist dieses Kontrollkästchen aktiviert, können Administratoren einen Filter zur Einschränkung der Organisationen angeben, die CA IdentityMinder nach einem Objekt durchsucht. Sie können Standardwerte für den Organisationssuchfilter angeben, indem Sie im Feld "Organisationssuche" ein Suchfenster angeben.

Organisationssuche speichern

Gibt an, dass die Organisation für die Aufgabe gespeichert wird, wenn eine Organisation für die Suche definiert wurde. Wenn ein Benutzer das nächste Mal einen Suchvorgang in der Aufgabe durchführt, wird die Organisation angezeigt.

Organisationssuche

Gibt das Suchfenster an, das CA IdentityMinder verwendet, um Administratoren die Suche nach einer Organisation zu gestatten.

Standardorganisationssuchbereich

Gibt den Standardorganisationssuchbereich an, der angezeigt wird, wenn ein Administrator ein Suchfenster nutzt. Der Suchbereich bestimmt die Ebenen in der Struktur einer Organisation, die in die Suchen einbezogen werden. Administratoren können den Standardorganisationssuchbereich überschreiben, indem sie im Suchfenster andere Suchkriterien angeben.

Wenn Sie beispielsweise in einer Umgebung, in der Auftragnehmerinformationen an verschiedenen Ebenen in der Organisationsstruktur gespeichert sind, ein Suchfenster für eine benutzerdefinierte Aufgabe "Auftragnehmer ändern" konfigurieren, können Sie für den Standardorganisationssuchbereich "und niedriger" einstellen.

Suche mit Einzelausdruck

Definiert die Art des Suchfilters, der im Suchfenster angezeigt wird. Ist dieses Kontrollkästchen aktiviert, können Benutzer einen einzelnen Suchfilter definieren, beispielsweise <attribut><komparator><wert>. Wenn Sie dieses Kontrollkästchen deaktivieren, können Benutzer mehrere Suchfilter angeben. Beispiel: <attribut1><komparator><wert1> AND <attribut2><komparator> <wert2>. Objekte, die die Bedingungen in sämtlichen Filtern erfüllen, werden in den Suchergebnissen zurückgegeben. Im obigen Beispiel würden Objekte mit <wert1> und <wert2> als Suchergebnisse zurückgegeben werden.

Nur mit Operator "Gleich" suchen

Verbietet Administratoren die Verwendung von anderen Suchoperatoren als "gleich".

Anzahl der Ergebnisse anzeigen

Zeigt die Anzahl der übereinstimmenden Suchergebnisse an. Wenn dieses Kontrollkästchen aktiviert ist, wird bei sämtlichen Suchvorgängen die Meldung "Es gibt x Ergebnisse" ausgegeben.

Schaltfläche "Aufgabe hinzufügen" für <aufgabenname>

Fügt dem Suchfenster eine Verknüpfung mit einer anderen Aufgabe hinzu. Die Verknüpfung wird in Form einer Schaltfläche angezeigt.
Dieses Feld dient normalerweise dazu, eine Aufgabe vom Typ "Erstellen" dem Suchfenster hinzuzufügen, die für die Objekt-Aufgabe-Navigation konfiguriert wurde.

Optionale Bezeichnung

Gibt eine Bezeichnung für die Aufgabe an, die Sie im vorherigen Feld ausgewählt haben. Diese Bezeichnung befindet sich auf der Schaltfläche für die Aufgabe.

Schaltfläche "Mehrfach löschen" hinzufügen für <aufgabenname>

Fügt einer Aufgabe eine Verknüpfung hinzu, über die Administratoren mehrere Objekte zum Löschen auswählen können. Die Verknüpfung wird in Form einer Schaltfläche angezeigt.
Dieses Feld kommt normalerweise bei der Objekt-Aufgaben-Navigation zum Einsatz.

Suchfelder und Suchergebnisse

In einem anderen Bereich des Suchfensters wählen Sie Felder, die ein Administrator in einer Suchabfrage verwenden sowie Felder aus, die in Suchergebnissen angezeigt werden sollen.

Felder auswählen, nach denen der Benutzer suchen kann

Wählen Sie die Felder aus, mit deren Hilfe ein Administrator eine Suchabfrage erstellen kann.

Wenn Sie weitere Felder hinzufügen möchten, wählen Sie die Felder im Listenfeld unterhalb der Tabelle mit den Suchfeldern aus.

Nachdem Sie die Felder ausgewählt haben, können Sie die Reihenfolge ändern, in der sie angezeigt werden. Verwenden Sie hierzu die Pfeil-nach-oben- bzw. Pfeil-nach-unten-Symbole rechts neben dem Feld.

Hinweis: Wenn Sie keine Felder angeben, die ein Administrator bei der Suche heranziehen kann, startet CA IdentityMinder den Suchvorgang automatisch.

Felder auswählen, die in den Suchergebnissen angezeigt werden

Wählen Sie die Felder aus, die CA IdentityMinder in den Suchergebnissen anzeigt. Sie können Felder auswählen, die in der Suchabfrage nicht zur Verfügung stehen.

Wenn Sie weitere Felder hinzufügen möchten, wählen Sie die Felder im Listenfeld unterhalb der Tabelle mit den Suchfeldern aus.

Formatvorlage

Wenn Sie ein Feld zur Anzeige in den Suchergebnissen auswählen, können Sie sich für eine der folgenden Formatvorlagenoptionen entscheiden:

- **Boolescher Anzeigename**

  Zeigt den Namen des Feldes für alle zutreffenden Ergebnisse an. Wenn Sie beispielsweise "Aktiviert" als den Namen des Attributs eingeben, das Aufschluss über den Kontostatus des Benutzers gibt, wird "Aktiviert" in den Suchergebnissen aller aktiven Benutzerkonten angezeigt.

- **Häkchen**

  Zeigt den Wert als aktiviertes Häkchen an, basierend auf dem Wert des Attributs. Wenn Sie beispielsweise das Häkchen zur Darstellung des Aktiviert-/Deaktiviert-Status von Benutzerkonten auswählen, zeigt CA IdentityMinder für sämtliche aktiven Konten ein aktiviertes Häkchen an.

- **Mehrwertige Zeichenfolge**

  Zeigt die Werte eines Attributs mit mehreren Werten in separaten Zeilen an. Die Werte werden in alphabetischer Reihenfolge aufgeführt.

- **Kontrollkästchen "Schreibgeschützt"**

  Zeigt den Wert als schreibgeschütztes Kontrollkästchen an.

- **Zeichenfolge**

  Zeigt den Wert als Textzeichenfolge an.

- **Aufgabe**

  Fügt einem Feld eine Aufgabenliste hinzu. Die Benutzer klicken auf ein Pfeil-Symbol, um eine Liste mit Aufgaben anzuzeigen, die sie für das mit dem Suchfeld verknüpfte Objekt durchführen können. Wenn Sie beispielsweise eine Aufgabenliste einem Feld mit der Bezeichnung "Nachname" in den Suchergebnissen hinzufügen, können die Benutzer auf das Pfeilsymbol in diesem Feld klicken, um eine Liste der Aufgaben anzuzeigen, die sie für den von ihnen ausgewählten Benutzer durchführen können.

  Diese Einstellung eignet sich auch, um einen Attributwert als Link auf eine Aufgabe anzuzeigen.

  Wenn Sie die Formatvorlage "Aufgabe" auswählen, wird neben der Spalte "Formatvorlage" ein Pfeil-nach-rechts-Symbol angezeigt. Klicken Sie auf den Pfeil, um ein Dialogfeld mit Feldeigenschaften zu öffnen. Nutzen Sie dieses Dialogfeld zur Konfiguration einer Aufgabenliste.

- **Aufgabenliste**

  Fügt zusätzliche Aufgaben hinzu, die Benutzer für Objekte in Such- und Listenfenstern durchführen können. Zum Beispiel können Sie das Suchfenster in der Aufgabe "Benutzer ändern" konfigurieren, um Benutzern zu ermöglichen, eine Aufgabe in der Liste von Benutzern, die von der Suche zurückgegeben wurden, durchzuführen, wie beispielsweise einen Benutzer zu deaktivieren.

  Wenn Sie diese Option auswählen, entscheiden Sie, ob Benutzer auf die Aufgabe zugreifen, indem sie auf ein Symbol oder einen Textlink klicken.

- **Aufgabenmenü**

  Fügt zusätzliche Aufgaben (ähnlich dem Aufgabenlisten-Stil) als Pop-up-Menü-Elemente hinzu.

  Wenn Sie diese Option auswählen, wird eine Aktionsschaltfläche neben jedem Objekt in einem Such- oder Listenfenster angezeigt. Benutzer klicken auf die Aktionsschaltfläche, um die Liste von Aufgaben anzuzeigen, die sie für dieses Objekt ausführen können.

Hinweis: Um die Formatvorlagenoptionen für die Aufgabenliste und das Aufgabenmenü anzuzeigen, wählen Sie (Trennzeichen) aus, wenn Sie ein Feld zur Suchergebnistabelle hinzufügen. Weitere Informationen dazu, wie Sie zusätzliche Aufgaben zu Such- und Listenfenstern hinzufügen, finden Sie im *Benutzerkonsolen-Designhandbuch*.

Sortierbar

Aktivieren Sie dieses Kontrollkästchen, um es Administratoren zu ermöglichen, Suchergebnisse anhand eines oder mehrerer Felder zu sortieren.

Standardsortierreihenfolge für Suchergebnisse festlegen

Gibt die Reihenfolge an, in der Suchergebnisse angezeigt werden. Anfänglich werden Suchergebnisse anhand des ersten Feldes in der Liste und dann anhand jedes weiteren Feldes sortiert, und zwar in der Reihenfolge, in der die Felder angezeigt werden. Aktivieren Sie das Kontrollkästchen "Absteigend", um Ergebnisse in absteigender Reihenfolge zu sortieren.

Objekte auswählen mit Änderungen in Feld *Feldname*

Legt fest, dass Objekte, in denen das angegebene Feld geändert wurde, ausgewählt werden, wenn der Benutzer auf die Schaltfläche "Auswählen" klickt.

***N* Ergebnisse pro Seite zurückgeben**

Wählen Sie die Anzahl der Ergebnisse aus, die pro Seite angezeigt werden sollen. Wenn die Suchergebnisse die von Ihnen angegebene Anzahl übersteigen, zeigt CA IdentityMinder eine Verknüpfung mit den einzelnen Ergebnisseiten an.

Benutzerdefinierte Hilfe in Suchfenstern

Wenn Sie Ihr Suchfenster um benutzerdefinierten Text ergänzen möchten, können Sie ihn im entsprechenden HTML-(HyperText Markup Language-)Textfeld definieren. Text kann in folgenden Bereichen hinzugefügt werden:

- Am Anfang oder Ende der Seite
- Vor oder nach der Erstellung
- Vor oder nach den Ergebnissen

Arten von Suchfenstern

In Identity Manager sind folgende vorkonfigurierten Suchfenster enthalten:

Zugriffsrollensuchfenster

Im Zugriffsrollensuchfenster können Sie Suchfilter konfigurieren, mit deren Hilfe Zugriffsrollen ausfindig gemacht werden, die bestimmten Kriterien entsprechen.

Zugriffsaufgabensuchfenster

Im Zugriffsaufgabensuchfenster können Sie Suchfilter konfigurieren, mit deren Hilfe Zugriffsausgaben ausfindig gemacht werden, die bestimmten Kriterien entsprechen. Dieses Suchfenster dient dazu, nach einer Zugriffsaufgabe zu suchen, die angezeigt oder geändert werden soll. Außerdem kann hier einer Zugriffsrolle eine Aufgabe hinzugefügt werden.

Admin-Rollen-Suchfenster

Im Admin-Rollen-Suchfenster können Sie Suchfilter konfigurieren, mit deren Hilfe Admin-Rollen ausfindig gemacht werden, die bestimmten Kriterien entsprechen.

Admin-Aufgabe-Suchfenster

Im Admin-Aufgabe-Suchfenster können Sie Suchfilter konfigurieren, mit deren Hilfe Admin-Aufgaben ausfindig gemacht werden, die bestimmten Kriterien entsprechen. Dieses Suchfenster dient dazu, nach einer Admin-Aufgabe zu suchen, die angezeigt oder geändert werden soll. Außerdem kann hier einer Admin-Rolle eine Aufgabe hinzugefügt werden.

Suchfenster für Genehmigungen

Im Suchfenster für Genehmigungen können Sie die Anzeige konfigurieren, die oberhalb von Genehmigungsaufgaben eingeblendet wird.

Zertifizierungsbeginn-Benutzersuchfenster

Im Zertifizierungsbeginn-Benutzersuchfenster können Sie Suchfilter für die Suche nach Benutzern konfigurieren, bei denen die Zertifizierung zur Bedingung gemacht werden soll. Der Zertifizierungsstatus der ausgewählten Benutzer wird auf *Zertifizierung erforderlich* eingestellt.

Benutzerzertifizierungs-Suchfenster

Im Benutzerzertifizierungs-Suchfenster können Sie Suchfilter zur Suche nach Benutzern konfigurieren, bei denen die Zertifizierung erforderlich ist.

Delegierungssuchfenster

Im Delegierungssuchfenster können Sie Suchfilter konfigurieren, mit deren Hilfe weitere Benutzer ausfindig gemacht werden, die als Delegierte hinzugefügt werden sollen. Ein Delegierter ist ein anderer Benutzer, dem Sie vorübergehend die Erlaubnis zum Anzeigen und Auflösen Ihrer Workflow-Arbeitselemente erteilen können.

Aktivierungs-/Deaktivierungs-Benutzersuchfenster

Im Aktivierungs-/Deaktivierungs-Benutzersuchfenster können Sie Suchfilter zur Aktivierung/Deaktivierung von Benutzern konfigurieren, die bestimmten Kriterien entsprechen.

Zertifizierungsende-Benutzersuchfenster

Im Zertifizierungsende-Benutzersuchfenster können Sie Suchfilter zur Identifizierung von Benutzern konfigurieren, deren Zertifizierungszyklus abgeschlossen werden sollte.

Suchfenster für Endbenutzer-Lizenzvereinbarung

Im Suchfenster für Endbenutzer-Lizenzvereinbarung können Sie die Aufgabe "Selbstregistrierung" mit einer Seite konfigurieren, die für Ihre identitätsbasierte Anwendung spezifisch ist.

Suchfenster zum Durchsuchen und Korrelieren

Im Suchfenster zum Durchsuchen und Korrelieren können Sie Suchfilter für das Durchsuchen und Korrelieren von Definitionen konfigurieren, die bestimmten Kriterien entsprechen.

Feeder-Dateiupload-Suchfenster

Im Feeder-Dateiupload-Suchfenster können Sie nach der Feeder-Datei suchen, die hochgeladen werden soll. Eine Feeder-Datei dient der Automatisierung wiederholt durchgeführter Aktionen, die für eine große Anzahl an verwalteten Objekten durchgeführt werden.

Suchfenster für "Kennwort vergessen"/"Benutzer-ID vergessen"

Im Suchfenster für "Kennwort vergessen" können Sie die Aufgabe "Kennwort vergessen" so konfigurieren, dass Benutzer zur Eingabe von Informationen aufgefordert werden, mit denen ihre Identität bestätigt werden kann.

Gruppensuchfenster

Im Gruppensuchfenster können Sie Suchfilter für Gruppen konfigurieren, beispielsweise Gruppen in der Finanzorganisation.

Identitätsrichtliniensatz-Suchfenster

Im Identitätsrichtliniensatz-Suchfenster können Sie Suchfilter zur Suche nach Identitätsrichtliniensätzen konfigurieren, die bestimmten Kriterien entsprechen.

Logical-Attribute-Handler-Suchfenster

Im Logical-Attribute-Handler-Suchfenster können Sie Suchfilter zur Suche nach Logical-Attribute-Handler konfigurieren. Dieses Suchfenster dient dem Ausfindigmachen eines Logical-Attribut-Handlers, dessen Konfiguration angezeigt bzw. geändert werden soll.

Berichtsverwaltungssuchfenster

Im Berichtsverwaltungssuchfenster können Sie Suchfilter zur Suche nach einem Bericht konfigurieren, der angezeigt bzw. gelöscht werden soll.

Suchfenster für nicht zertifizierte Benutzer

Im Suchfenster für nicht zertifizierte Benutzer können Sie Suchfilter zur Suche nach Benutzern konfigurieren, die am Ende der Zertifizierungsperiode nicht zertifiziert waren.

Organisationssuchfenster

Im Organisationssuchfenster können Sie Suchfilter konfigurieren, mit deren Hilfe die Organisationsauswahl auf bestimmte Unterorganisationen beschränkt werden kann.

Bereitstellungsrollensuchfenster

Im Bereitstellungsrollensuchfenster können Sie die Suchfilter für das Abrufen von Bereitstellungsrollen konfigurieren.

Kontovorlagensuchfenster

Im Kontovorlagensuchfenster können Sie die Suchfilter für das Abrufen von Kontovorlagen konfigurieren.

Kennwortrichtliniensuchfenster

Im Kennwortrichtliniensuchfenster können Sie die Suchfilter zur Suche nach Kennwortrichtlinien konfigurieren, die bestimmten Kriterien entsprechen.

Snapshot-Definition-Suchfenster

Im Snapshot-Definition-Suchfenster können Sie die Suchfilter zur Suche nach einer Snapshot-Definition konfigurieren, die angezeigt, geändert oder gelöscht werden soll.

Standardsuchfenster

Im Standardsuchfenster können Sie Filter zur Suche nach benutzerdefinierten verwalteten Objekten konfigurieren.

Benutzersuchfenster

Im Benutzersuchfenster können Sie Suchfilter zur Suche nach Benutzern konfigurieren, die bestimmten Kriterien entsprechen. Sie können beispielsweise nach Benutzern suchen, die Auftragnehmer sind.

Nachdem Sie auf der Registerkarte "Suchen" alle erforderlichen Schritte durchgeführt haben, führen Sie den Schritt Auswählen von Registerkarten für Aufgaben durch.

Auswählen von Registerkarten für Aufgaben

Konfigurieren Sie die Registerkarten auf der Registerkarte "Registerkarten". Bei jeder Registerkarte handelt es sich um einen Satz von Feldern, den Sie in der Aufgabe einschließen. Sie können Standardregisterkarten verwenden oder neue erstellen. Die Aufgabe "Benutzer ändern" weist beispielsweise die folgenden Registerkarten auf:

- Profil
- Zugriffsrollen
- Admin-Rollen
- Gruppen
- Arbeitselemente delegieren

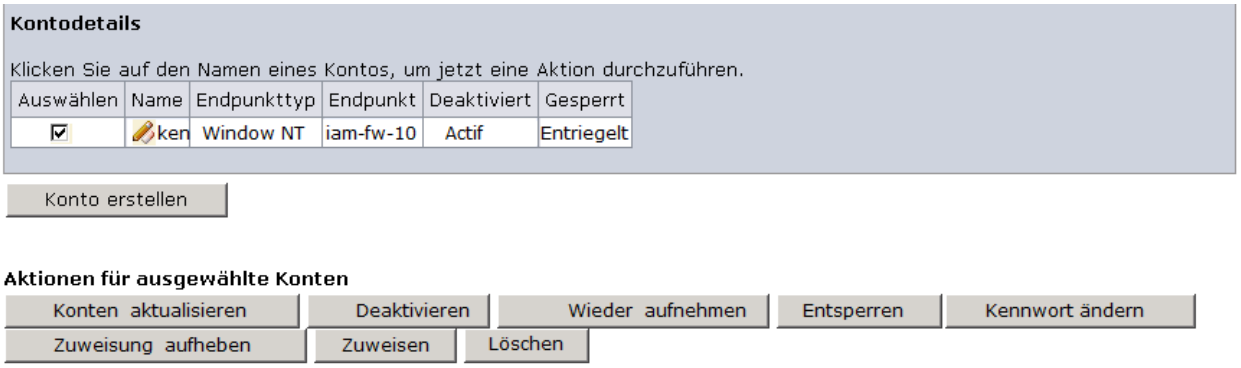
Um die Definition einer Registerkarte zu bearbeiten, klicken Sie auf das Bearbeitungssymbol ( ) neben dem Registerkartennamen.

Weitere Informationen:

Registerkarte "Konten" (siehe Seite 68)
Registerkarte "Ablaufplan" (siehe Seite 70)

Registerkarte "Konten"

Auf der Registerkarte "Konten" werden Konten auf verwalteten Endpunkten für Benutzer aufgeführt, denen Bereitstellungsrollen zugewiesen wurden. Normalerweise wird diese Registerkarte Aufgaben hinzugefügt, die Ihnen das Anzeigen oder Ändern eines Benutzers ermöglichen.



Wird die Registerkarte "Konten" einer Aufgabe vom Typ "Benutzer ändern" hinzugefügt, können Administratoren andere Aktionen für die Konten des jeweiligen Benutzers durchführen. Beispiel:

- Konto deaktivieren oder wieder aufnehmen.
- Konto entsperren, das aufgrund von falschem oder unangemessenem Zugriff automatisch gesperrt wurde. Ein Konto kann beispielsweise gesperrt werden, wenn ein Benutzer die akzeptable Anzahl an fehlgeschlagenen Anmeldeversuchen überschreitet, die in einer Kennwortrichtlinie in Identity Manager festgelegt wurde.
- Kennwort des Benutzers für ein oder mehrere Konten ändern.
- Konten einem Benutzer zuweisen bzw. die Zuweisung aufheben.

Einzelheiten zu den weiteren Optionen, die Sie auf der Registerkarte "Konten" angeben können, finden Sie in der Hilfe der Benutzerkonsole für die Registerkarte Konten konfigurieren.

Voraussetzung für die Verwendung der Registerkarte "Konten"

Um die Registerkarte "Konten" verwenden zu können, muss Identity Manager für die Bereitstellungsunterstützung konfiguriert sein und in der Identity Manager-Umgebung muss ein Bereitstellungsverzeichnis vorhanden sein.

Hinweis: Ziehen Sie hinsichtlich der Konfiguration für die Bereitstellungsunterstützung das *Konfigurationshandbuch* zurate.

Felder auf der Registerkarte "Konten"

Auf der Registerkarte "Konten" werden Details zu den Konten angezeigt, über die der Benutzer auf Endpunktsystemen verfügt.

Hier einige der wichtigeren Felder:

- Name: Anmeldename, E-Mail-Name oder anderer Name für das Konto.
- Endpunkttyp: Der Typ des Endpunkts (z. B. ein LDAP-Verzeichnis), das mit dem Konto verknüpft ist.
- Endpunkt: Der spezifische Endpunkt, der mit dem jeweiligen Konto verknüpft ist.
- Deaktiviert: Einer von drei Status.
  - "Aktiv" wird angezeigt, wenn das Konto aktiviert ist.
  - "Deaktiviert" wird angezeigt, wenn das Konto deaktiviert ist.
  - "Aktivierung steht aus (manuell)" wird angezeigt, wenn das Konto weder reaktiviert noch deaktiviert werden kann. Melden Sie sich beim Endpunkt-System an, um das Konto zu reaktivieren oder zu deaktivieren.
  - Wenn der Status nicht abgerufen werden kann, weil es keine Kommunikation mit dem Endpunkt gibt, wird "Nicht verfügbar" angezeigt.
- Gesperrt: Zeigt an, ob das Konto gesperrt ist. Die Sperrung erfolgt, wenn ein Benutzer mehrfach versucht, sich bei dem Konto mit einem falschen Kennwort anzumelden. Wenn der Status nicht abgerufen werden kann, weil es keine Kommunikation mit dem Endpunkt gibt, wird "Nicht verfügbar" angezeigt.

Zusätzliche Funktionen auf der Registerkarte "Konten"

Ist die Registerkarte "Konten" Bestandteil einer Aufgabe, mit der ein Benutzer geändert wird, können Administratoren mit Hilfe dieser Aufgabe Funktionen für die Konten des jeweiligen Benutzers durchführen. Welche Funktionen zur Verfügung stehen wird durch die Konfiguration der Registerkarte bestimmt.

Sie können auswählen, welche Funktionen verfügbar sind, indem Sie "Admin-Aufgabe ändern" auf eine Aufgabe mit der Registerkarte "Konten" ausführen. Sie bearbeiten die Registerkarte "Konten", um zu bestimmen, ob Funktionen, beispielsweise "Konto zuweisen" und "Kontozuweisung aufheben", auf der Registerkarte verfügbar sind.

Weitere Informationen finden Sie in der Online-Hilfe zur Registerkarte Konten konfigurieren.

Registerkarte "Ablaufplan"

Mit Hilfe von Ablaufplänen können Sie die Ausführung einer Aufgabe zu einem späteren Zeitpunkt automatisieren. Wenn Sie eine Aufgabe planen, die mit einem Workflow verknüpft ist, führt CA IdentityMinder sämtliche Aufgaben gemäß Definition in diesem Workflow aus.Der Status der geplanten Aufgaben kann auf der Seite "Gesendete Aufgaben anzeigen" eingesehen werden.

Eine geplante Aufgabe, die noch nicht von CA IdentityMinder ausgeführt wurde, kann über die Seite "Gesendete Aufgaben anzeigen" verworfen werden.

Hinweis: Wenn eine geplante Aufgabe verworfen wird, und Sie diese Aufgabe erneut senden, wird die Aufgabe unabhängig vom planmäßigen Ausführungszeitpunkt sofort ausgeführt.

In CA IdentityMinder wird der Scheduler als spezielle Registerkarte bereitgestellt. Um auf den Scheduler zugreifen zu können, müssen Sie eine Aufgabe über die Registerkarte "Ablaufplan" konfigurieren.

Hinzufügen der Registerkarte "Ablaufplan" zu Admin-Aufgaben

Mit CA IdentityMinder können Sie die Ausführung Ihrer Aufgaben für ein bestimmtes Datum und eine bestimme Uhrzeit planen. Um eine Aufgabe planen zu können, müssen Sie die Registerkarte "Ablaufplan" einer Admin-Aufgabe hinzufügen.

Hinweis: Es ist nicht möglich, sämtlichen Admin-Aufgaben in CA IdentityMinder eine Registerkarte vom Typ "Ablaufplan" hinzuzufügen. Wenn die Aufgabe nicht geplant werden kann, steht die Registerkarte "Ablaufplan" im Fenster "Admin-Aufgabe ändern" nicht zur Verfügung.

So fügen Sie die Registerkarte "Ablaufplan" zu Admin-Aufgaben hinzu:

1. Klicken Sie auf "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe ändern".

   Daraufhin wird die Seite "Admin-Aufgabe auswählen" angezeigt.

2. Wählen Sie im Feld "Admin-Aufgaben durchsuchen" die Option "Name" oder "Kategorie" aus, geben Sie die zu suchende Zeichenfolge ein, und klicken Sie dann auf "Suchen".

   Daraufhin werden in CA IdentityMinder die Admin-Aufgaben angezeigt, die den Suchkriterien entsprechen.

3. Wählen Sie eine Admin-Aufgabe aus, und klicken Sie dann auf "Auswählen".

   Daraufhin werden in CA IdentityMinder die Aufgabendetails der ausgewählten Admin-Aufgabe angezeigt.

4. Klicken Sie auf "Registerkarten".

   Daraufhin werden die Registerkarten angezeigt, die für die ausgewählte Admin-Aufgabe konfiguriert sind.

5. Wählen Sie auf den Registerkarten, die in dieser Dropdown-Liste angezeigt werden sollen, die Option "Ablaufplan" aus, und klicken Sie dann auf " ".

   Die Registerkarte "Ablaufplan" wird der Liste der Registerkarten hinzugefügt, die in der ausgewählten Admin-Aufgabe angezeigt werden.

6. Klicken Sie auf "Senden".

   Daraufhin wird die Registerkarte "Ablaufplan" der ausgewählten Admin-Aufgabe hinzugefügt.

Anzeigen von Feldern in Aufgaben

Auf der Registerkarte "Felder" können Sie die Felder anzeigen, die für diese Aufgabe relevant sind. Bei diesen Feldern handelt es sich um diejenigen, die auf den Registerkarten für diese Aufgabe erstellt wurden. Wenn andere Felder verwendet werden sollen, kehren Sie zur Registerkarte "Registerkarten" zurück, und klicken Sie auf die Registerkarte, die geändert werden muss.

Nachdem Sie auf dieser Registerkarten die erforderlichen Schritte durchgeführt haben, fahren Sie mit dem nächsten Schritt fort, Zuweisen von Workflow-Prozessen für Ereignisse (siehe Seite 72).

In dieser Identity Manager-Umgebung kommen jedoch keine Workflows zum Einsatz, Sie können also jetzt auf "Senden" klicken. Daraufhin wird eine Meldung ausgegeben, aus der hervorgeht, ob die Aufgabe erfolgreich durchgeführt wurde. Ist dies der Fall, können Sie die Aufgabe einer Rolle hinzufügen, damit die Rollenmitglieder mit der Aufgabe arbeiten können.

Rollenverwendung anzeigen

Auf dieser Registerkarte werden die Rollen angezeigt, zu denen die Aufgabe gehört, die Sie anzeigen oder ändern.

Rolleneigentümer können Aufgaben zu Rollen hinzufügen oder daraus entfernen.

Hinweis: <Unter Standard-Admin-Rollen finden Sie eine Liste der Admin-Rollen, die standardmäßig mit CA IdentityMinder installiert werden.

Zuweisen von Workflow-Prozessen für Ereignisse

Wenn Sie die Workflow-Funktion für diese Identity Manager-Umgebung aktiviert haben, wählen Sie auf der Registerkarte "Ereignisse" einen Workflow-Prozess für sämtliche Ereignisse aus, die von der Aufgabe initiiert werden. Der von Ihnen ausgewählte Workflow-Prozess setzt denjenigen außer Kraft, der in der Identity Manager-Management-Konsole standardmäßig ausgewählt ist.

Weitere Details zu standardmäßigen Workflow-Zuordnungen finden Sie im *Konfigurationshandbuch* im Kapitel zu den erweiterten Einstellungen.

Klicken Sie auf "Senden", um die Erstellung dieser Aufgabe abzuschließen. Daraufhin wird eine Meldung ausgegeben, aus der hervorgeht, ob die Aufgabe erfolgreich durchgeführt wurde. Ist dies der Fall, können Sie die Aufgabe einer Rolle hinzufügen, damit die Rollenmitglieder mit der Aufgabe arbeiten können.

Verwalten eines Active Directory-Benutzerspeichers

Wenn Active Directory der Benutzerspeicher ist, müssen Sie vor dem Erstellen von Admin-Aufgaben möglicherweise bestimmte Active Directory-Funktionen konfigurieren.

Attribut "sAMAccountName"

Das Attribut "sAMAccountName" bezieht sich auf Benutzer und Gruppen. Dieses Attribut ist erforderlich und muss in Aufgabenfenstern für das Erstellen von Benutzern und Gruppen vorhanden sein.

Hinweis: Beim Erstellen von Benutzern darf der Wert des sAMAccountName-Attributs höchstens 20 Zeichen umfassen. Diese Einschränkung gilt nicht für Gruppen.

Sie können einen benutzerdefinierten Logical-Attribute-Handler schreiben, der beim Erstellen eines Benutzers oder einer Gruppe automatisch ein eindeutiges sAMAccountName-Attribut erstellt. In diesem Fall können Sie das sAMAccountName-Attribut als verborgenes Feld in die Fenster "Benutzer erstellen" und "Gruppe erstellen" aufnehmen.

Weitere Informationen finden Sie im *Programmierhandbuch für Java* im Kapitel zu logischen Attributen.

Gruppentyp und Bereich

In Active Directory gibt es zwei Arten von Gruppen:

- Sicherheit: Aufgeführt in Zugriffssteuerungslisten (Access Control Lists, ACLs), mit deren Hilfe Berechtigungen für Ressourcen und Objekte definiert werden.
- Verteilung: Dient der Gruppierung von Objekten, etwa Benutzern und Gruppen. Verteilungsgruppen können in Active Directory nicht zur Erteilung von Berechtigungen verwendet werden.

Jede Art von Gruppe weist einen Bereich auf, mit dem Folgendes bestimmt wird:

- Mitgliedsspeicherort: Der Ort, an dem sich potenzielle Mitglieder befinden können.
- Berechtigungen: Wo die Gruppe für Zugriffsberechtigungen verwendet werden kann (wenn es sich bei der Gruppe um eine Sicherheitsgruppe handelt).
- Gruppenmitgliedschaft in anderen Gruppen: Der Speicherort von Gruppen, denen die Gruppe zugehörig sein kann.

Jede Art von Gruppe kann einen der folgenden Bereiche aufweisen:

Bereich	Mitgliedsspeicherort	Berechtigungen	Gruppenmitgliedschaft in anderen Gruppen
Universal	Gruppenmitglieder können universelle Gruppen, globale Gruppen sowie Benutzer aus einer beliebigen Domäne in der Struktur sein.	Können zur Gewährung von Zugriff in sämtlichen Domänen einer Struktur verwendet werden.	Können Mitglieder in domänenlokalen und universellen Gruppen in beliebigen Domänen der Struktur sein.
Global	Gruppenmitglieder können globale Gruppen sowie Benutzer aus derselben Domäne wie die Gruppe sein.	Können zur Gewährung von Zugriff in sämtlichen Domänen einer Struktur verwendet werden.	Können Mitglieder in globalen, domänenlokalen und universellen Gruppen in beliebigen Domänen der Struktur sein.
Domänenlokal	Gruppenmitglieder können universelle Gruppen, globale Gruppen sowie Benutzer aus einer beliebigen Domäne in der Struktur sein. Mitglieder können zudem domänelokale Gruppen aus derselben Domäne sein.	Können nur zur Gewährung von Zugriff auf die Domäne verwendet werden, in der sich die Gruppe befindet.	Können nur Mitglieder anderer domänenlokaler Gruppen in der Domäne sein.

Gruppentyp und Bereich sind keine erforderlichen Attribute, wenn Sie jedoch keinen Gruppentyp und Bereich angeben, erstellt Active Directory eine Sicherheitsgruppe mit globalem Bereich.

Wenn Sie Gruppen eines anderen Typs erstellen möchten, können Sie einen benutzerdefinierten Logical-Attribute-Handler erstellen. Ziehen Sie das Kapitel zu logischen Attributen im *Programmierhandbuch für Java* zurate.

Nachdem Sie diese Active Directory-Funktionen konfiguriert haben, fahren Sie mit dem nächsten Schritt fort: Erstellen von Admin-Aufgaben.

Externe Aufgaben für Anwendungsfunktionen

Eine externe Aufgabe bewirkt Folgendes:

- Ermöglicht es einem Administrator, über die Benutzerkonsole von Identity Manager eine Funktion in einer anderen Anwendung als CA IdentityMinder durchzuführen
- Optional werden Informationen zur Anwendung übergeben, um benutzer-, gruppen- oder organisationsspezifische Aufgaben zu generieren.

Zum Beispiel kann eine externe Aufgabe Informationen zu einer Organisation an eine Anwendung übergeben, die Aufträge generiert. Der Administrator, der die Aufgabe durchführt, kann über die Benutzerkonsole offene Aufträge für die Organisation anzeigen.

Sie können externe Aufgaben anzeigen, indem Sie die Anwendung in einem neuen Browserfenster öffnen oder sie als Registerkarten in einer CA IdentityMinder-Admin-Aufgabe anzeigen.

Zwei Registerkarten sind für externe Aufgaben verfügbar. Diese Registerkarten werden auf gleiche Weise konfiguriert. Allerdings funktionieren sie anders.

- Die Registerkarte "Extern" ist eine visuelle Registerkarte. Das heißt, dass die Aufgabe die Inhalte der URL innerhalb einer Registerkarte anzeigt.
- "Externer URL" ist eine nicht-visuelle Registerkarte. Das heißt, dass die Aufgabe zur eingegebenen URL umgeleitet wird.

Die Registerkarte "Extern"

Zu jeder Erstellungs-, Anzeige- und Änderungsaufgabe kann eine externe Registerkarte hinzugefügt werden, um die Aufgabe zu einer externen Aufgabe zu machen. Wenn Sie beispielsweise die Registerkarte "Extern" zur Aufgabe "Benutzer erstellen" hinzufügen, wird die Registerkarte für diese Aufgabe angezeigt.

Für die Registerkarte "Extern" gilt Folgendes:

- Für eine externe Aufgabe werden keine Ereignisse generiert.
- Sie können optional verwaltete Objekte verwenden.
- Im Feld "Externe URL" können Sie die Adresse der Anwendung wie folgt angeben:
  - Als vollständige Adresse, einschließlich des vollständig qualifizierten Domänennamens, zum Beispiel:

    http://server1.mycompany.org/report/viewUserReport
  - Als relativen Pfad, zum Beispiel:

    /report/viewUserReport

    Wenn Sie den relativen Pfad angeben, fügt CA IdentityMinder automatisch den vollständig qualifizierten Domänennamen des Servers an, auf dem CA IdentityMinder installiert ist.
- Sie konfigurieren die Attribute, die auf der Registerkarte "Profil" an die Anwendung übergeben werden.
- Sie können den Admin-DN oder Aufgabennamen in der URL angeben oder nicht einschließen.

Die Registerkarte "Externe URL"

Sie können die Registerkarte "Externe URL" zu einer Anzeigeaufgabe, z. B. "Benutzer anzeigen", hinzufügen. Wenn Sie die Aufgabe "Benutzer anzeigen" verwenden, werden Sie an die durch die URL identifizierte Website umgeleitet. Es werden keine anderen Registerkarten angezeigt.

Für die Registerkarte "Externe URL" gilt Folgendes:

- Die Registerkarte "Externe URL" muss die einzige Registerkarte in der Aufgabe sein. Wenn andere Registerkarten der gleichen Aufgabe zugeordnet sind, werden Benutzer von der Registerkarte "Externe URL" nicht an die angegebene URL umgeleitet.
- Die Aufgabe kann Ereignisse generieren, die geprüft werden können.

- Im Feld "Externe URL" können Sie die Adresse der Anwendung wie folgt angeben:
  - Als vollständige Adresse, einschließlich des vollständig qualifizierten Domänennamens, zum Beispiel:

    http://server1.mycompany.org/report/viewUserReport
  - Als relativen Pfad, zum Beispiel:

    /report/viewUserReport

    Wenn Sie den relativen Pfad angeben, fügt CA IdentityMinder automatisch den vollständig qualifizierten Domänennamen des Servers an, auf dem CA IdentityMinder installiert ist.
- Sie können optional verwaltete Objekte verwenden.
- Sie können Attribute konfigurieren, die an die URL übergeben werden.

  Geben Sie eine URL für die Anwendung an, die gestartet werden soll, und schließen Sie die Attribute ein, die Sie an die Anwendung übergeben möchten.
- Sie können den Admin-DN oder Aufgabennamen in der URL angeben oder nicht einschließen.

Erweiterte Aufgabenkomponenten

Erweiterte Aufgabenkomponenten ermöglichen es Ihnen, benutzerdefinierte Verarbeitung für eine Aufgabe anzugeben:

- Aufgabenebenen-Validierung validiert einen Attributwert gegenüber anderen Attributen in der Aufgabe. Sie können zum Beispiel validieren, ob die Ortsnetzkennzahl in einer vom Benutzer bereitgestellten Telefonnummer der Stadt und dem Land des Benutzers entspricht.
- Business Logic Task-Handler (siehe Seite 77) führt benutzerdefinierte Business Logic aus, bevor eine CA IdentityMinder-Aufgabe zur Verarbeitung übergeben wird. Normalerweise validiert die benutzerdefinierte Business Logic die Daten. Zum Beispiel kann ein Business Logic Task-Handler die Mitgliedschaftsbeschränkung überprüfen, bevor CA IdentityMinder der Gruppe ein neues Mitglied hinzufügt. Wenn die Gruppenmitgliedschaftsbeschränkung erreicht wird, zeigt der Business Logic Task-Handler eine Meldung an, die den Gruppenadministrator darüber informiert, dass das neue Mitglied nicht hinzugefügt werden konnte.

Erstellen von Business Logic Task-Handler

Gehen Sie zur Definition des voll qualifizierten Klassennamens eines Business Logic Task-Handler folgendermaßen vor:

1. Erstellen oder ändern Sie eine Admin-Aufgabe.
2. Klicken Sie auf der Registerkarte für das Administratorprofil auf "Business Logic Task-Handler".

   Daraufhin wird das Fenster "Business Logic Task-Handler" angezeigt. In diesem Fenster werden alle vorhandenen Business Logic Task-Handler aufgeführt, die der Aufgabe zugewiesen sind. Identity Manager führt die Handler in der Reihenfolge aus, in der sie in der Liste angegeben sind.
3. Klicken Sie auf "Hinzufügen".

   Daraufhin wird das Fenster "Business Logic Task Handler: Detail" angezeigt.

Definieren Sie im Fenster "Business Logic Task Handler: Detail" folgende Informationen für den Business Logic Task-Handler, den Sie der Aufgabe zuweisen:

Name

Der Name, den Sie dem Business Logic Task-Handler zuweisen.

Beschreibung

Eine optionale Beschreibung des Business Logic Task-Handlers.

Java-Klasse

Wenn der Business Logic Task-Handler in Java implementiert ist, der voll qualifizierte Klassenname des Business Logic Task-Handlers. Beispiel:

com.mycompany.MyJavaBLTH

Identity Manager geht davon aus, dass sich die Klassendatei im Stammverzeichnis für benutzerdefinierte Java-Klassendateien befindet. Informationen zur Bereitstellung von Java-Klassendateien finden Sie im *Programmierhandbuch für Java*.

JavaScript-Dateiname

Wenn der Business Logic Task-Handler in JavaScript implementiert und der JavaScript-Code in einer Datei enthalten ist, geben Sie in diesem Feld den Dateinamen an. Wenn der Business Logic Task-Handler von mehreren Aufgabenfenstern verwendet werden soll, empfiehlt es sich beispielsweise, den JavaScript-Code in einer Datei zu speichern.

Identity Manager geht davon aus, dass sich die Datei im Stammverzeichnis für benutzerdefinierte JavaScript-Dateien befindet. Informationen zur Bereitstellung von JavaScript-Dateien finden Sie im *Programmierhandbuch für Java*.

Wenn Sie die Datei in einem Unterverzeichnis des Stammverzeichnisses speichern, geben Sie beim Angeben des Namens der JavaScript-Datei auch den Namen des Unterverzeichnisses an. Beispiel:

JavaScriptSubDir\MyJavaScriptBLTH.js

Die Schrägstriche müssen der Plattform entsprechen, auf der die JavaScript-Datei bereitgestellt wird.

JavaScript

Sie können einen JavaScript-Business Logic Task-Handler implementieren, indem Sie den vollständigen JavaScript-Code in diesem Feld anstatt in einer Datei angeben. So empfiehlt es sich beispielsweise, den JavaScript-Code in diesem Feld anzugeben, wenn das Script sehr kurz ist bzw. für keine anderen Aufgabenfenster zum Einsatz kommt.

"Eigenschaft" und "Wert"

Bei Java-Implementierungen handelt es sich bei diesen Feldern um optionale Name/Wert-Paare, die an die init()-Methode des Java-Business Logic Task-Handler übergeben und auf jede beliebige Weise verwendet werden, die die Geschäftslogik (Business Logic) des Handlers erforderlich macht.

Wenn Sie eine benutzerdefinierte Eigenschaft hinzufügen möchten, geben Sie einen Eigenschaftsnamen und -wert an, und klicken Sie dann auf "Hinzufügen".

Hinweis: Wenn Sie einen Java-Business Logic Task-Handler hinzufügen, starten Sie den Anwendungsserver neu, damit der Handler geladen wird.

Admin-Aufgaben und Ereignisse

Admin-Aufgaben beinhalten *Ereignisse*. Hierbei handelt es sich um Aktionen, die von CA IdentityMinder zum Abschließen von Aufgaben ausgeführt werden. Eine Aufgabe kann mehrere Ereignisse umfassen. So kann beispielsweise die Aufgabe "Benutzer erstellen" Ereignisse für das Erstellen des Benutzerprofils, das Hinzufügen des Benutzers zu einer Gruppe und das Zuweisen von Rollen beinhalten.

CA IdentityMinder überprüft Ereignisse, setzt kundenspezifische Geschäftsregeln für die Ereignisse durch und fordert die Bestätigung der Ereignisse an, falls diese Workflow-Prozesse zugeordnet sind.

Falls für eine Aufgabe mehrere Ereignisse generiert werden und diese Ereignisse Workflow-Prozessen zugeordnet sind, müssen alle Workflow-Prozesse abgeschlossen sein, bevor CA IdentityMinder die Aufgabe abschließen kann.

Primäre und sekundäre Ereignisse

In der Regel ist ein Ereignis nicht von anderen Ereignissen abhängig. Allerdings sind einige Aufgaben einem primären und einem oder mehreren sekundären Ereignissen zugeordnet:

- Der Fehlschlag eines primären Ereignisses führt zur automatischen Ablehnung aller sekundären Ereignisse. Wenn beispielsweise das Ereignis "CreateUserEvent" fehlschlägt, muss für den Benutzer auch das Ereignis "AddToGroupEvent" nicht eintreten. Außerdem wird die zugeordnete Aufgabe storniert.
- Der Fehlschlag eines sekundären Ereignisses beeinträchtigt nicht den Erfolg oder Misserfolg eines anderen Ereignisses, das für die Aufgabe durchgeführt wird, und nicht die Ausführung der Aufgabe selbst. Wenn beispielsweise in der Aufgabe "Benutzer erstellen" das Ereignis "AddToGroupEvent" abgelehnt wird, hat dies zur Folge, dass der neue Benutzer nicht einer bestimmten Gruppe hinzugefügt werden kann. Dennoch kann der Benutzer erstellt (CreateUserEvent), Bereitstellungsrollen zugeordnet werden (AssignProvisioningRoleEvent) und sogar anderen Gruppen hinzugefügt werden.

Ereignisse für eine Aufgabe anzeigen

Sie können in CA IdentityMinder die Ereignisse anzeigen, die mit einer Aufgabe verknüpft sind.

So zeigen Sie Ereignisse für eine Aufgabe an

1. Wählen Sie in der Benutzerkonsole "Rollen und Aufgaben", "Admin-Aufgabe anzeigen" aus.
2. Suchen Sie nach der entsprechenden Aufgabe, und wählen Sie sie aus.
3. Wählen Sie die Registerkarte Ereignisse aus.

   CA IdentityMinder zeigt die Ereignisse an, die der aktuellen Aufgabe zugeordnet sind.

Für nicht geänderte Profile generierte Ereignisse

Benutzer, Gruppen und Organisationsobjekte enthalten jeweils einen Satz physischer Attribute, die im Benutzerverzeichnis gespeichert werden. Wenn ein physisches Attribut eines dieser Objekte auf einer Profilregisterkarte geändert wird, generiert Identity Manager ein Modify-Ereignis, nachdem der Benutzer die Aufgabe sendet. Wenn z. B. das Attribut *Titel* auf der Registerkarte "Benutzerprofil" geändert wird, generiert Identity Manager das ModifyUserEvent-Ereignis.

Wenn ein Benutzer, eine Gruppe oder ein Organisationsobjekt auf einer Profilregisterkarte repräsentiert wird, aber keine physischen Attribute geändert wurden, und der Benutzer auf "Senden" klickt, dann wird von Identity Manager kein Modify-Ereignis erstellt. Stattdessen wird das entsprechende View-Ereignis wie folgt generiert:

- ViewUserEvent wird anstelle von ModifyUserEvent erstellt
- ViewGroupEvent wird anstelle von ModifyGroupEvent erstellt
- ViewOrganizationEvent wird anstelle von ModifyOrganizationEvent erstellt

Verarbeiten von Admin-Aufgaben

Die Zeit, die zum Verarbeiten von Aufgaben erforderlich ist, hängt von den enthaltenen Schritten ab. Wenn Aufgaben zum Verarbeiten gesendet werden, führt CA IdentityMinder folgende Schritte aus:

1. CA IdentityMinder überprüft die übermittelten Daten.

   Dies wird als *synchrone Phase* bezeichnet.

2. Falls für die Aufgabe eine Genehmigung erforderlich ist, sendet CA IdentityMinder die Aufgabe an die Workflow-Engine.

   a. Die Workflow-Engine bestimmt die Genehmiger und legt die Genehmigungsaufgabe in der Arbeitsliste des Genehmigers ab.

   b. Optional kann CA IdentityMinder eine E-Mail versenden, die die Genehmiger über das ausstehende Arbeitselement benachrichtigt.

   c. Ein Genehmiger reserviert das Arbeitselement (wodurch das Element aus der Arbeitsliste anderer Genehmiger entfernt wird) und genehmigt das Element oder lehnt es ab.

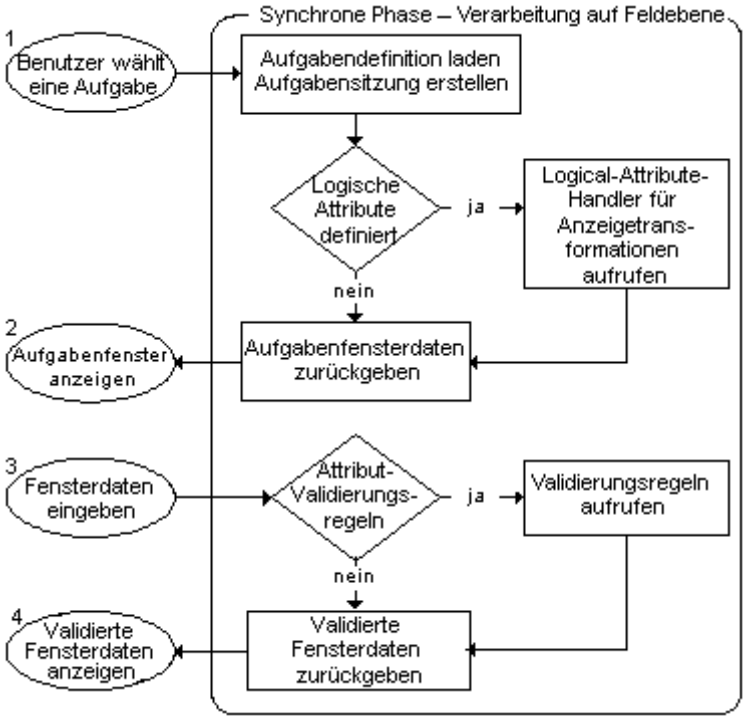
   d. Optional kann CA IdentityMinder eine E-Mail versenden, die die beteiligten Benutzer über den Status der Aufgabe benachrichtigt.

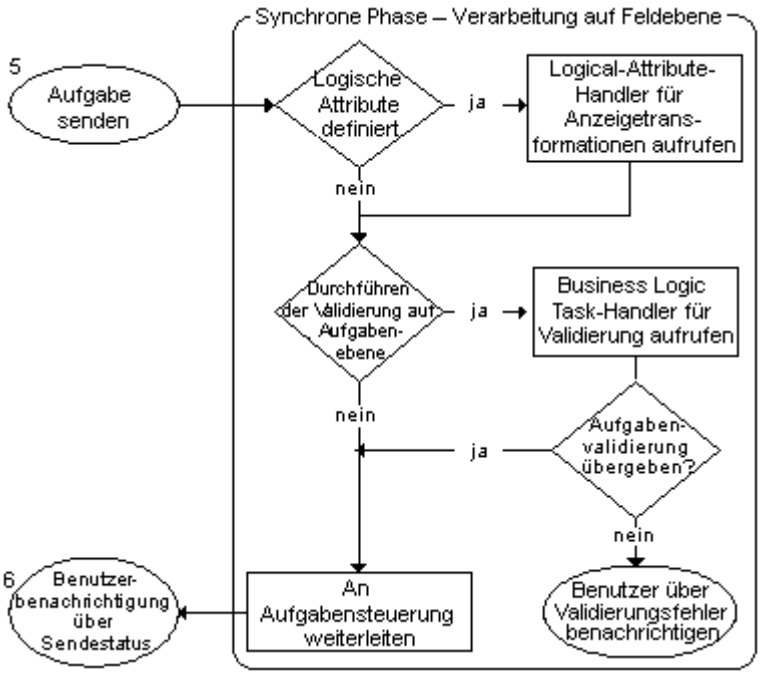
   Dies wird als *asynchrone Phase* bezeichnet.

3. CA IdentityMinder führt die Aufgabe aus, falls diese nicht abgelehnt wurde.

Verarbeitung – synchrone Phase

Während der synchronen Phase kann Identity Manager Daten, die Benutzer in Aufgabenfenstern eingeben, umwandeln und überprüfen und die Anwendung von Business-Logik auf diese Daten erzwingen, bevor die Aufgabe verarbeitet wird. In der folgenden Abbildung finden Sie einen Überblick darüber, was während dieser Phase geschieht.

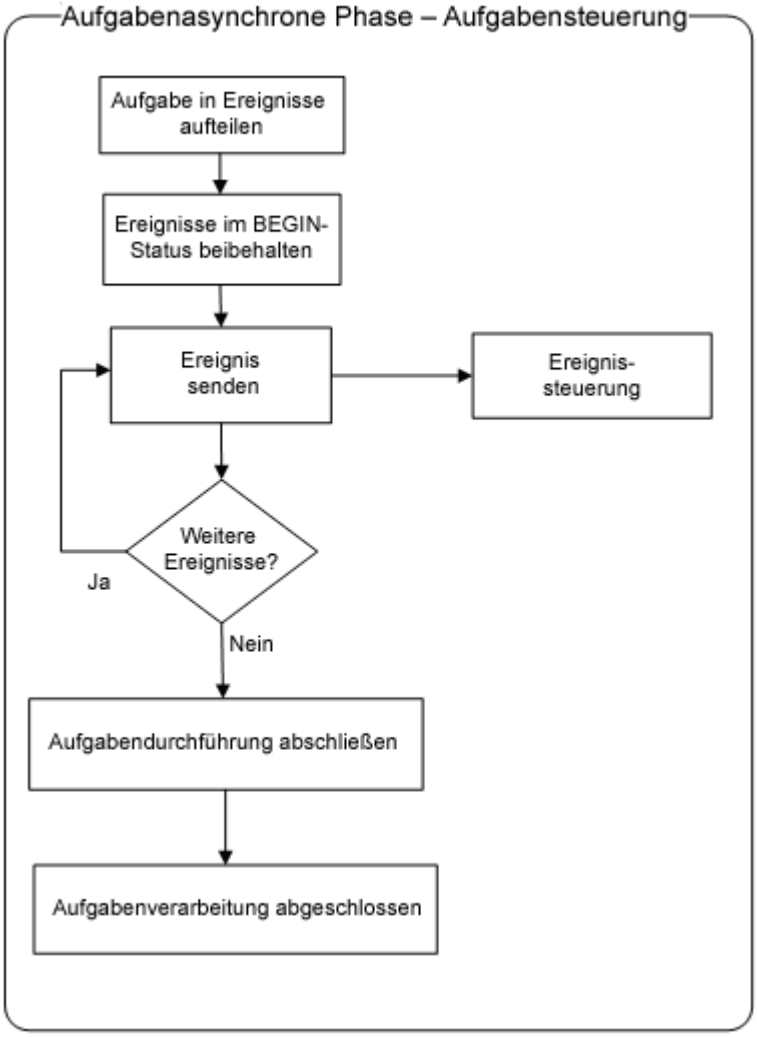




Verarbeitung – asynchrone Phase

Bei Beendigung der synchronen Phase tritt die Aufgabe zur Ausführung in die asynchrone Phase ein. Während dieser Phase erzeugt die Aufgabe ein oder mehrere Ereignisse. Dabei kann es sich um benutzerdefinierte Ereignisse, beispielsweise das Erstellen eines Benutzerprofils oder das Hinzufügen eines Benutzers zu einer Gruppe, oder um vom System erzeugte Ereignisse, wie das Schreiben von Informationen in das Audit-Protokoll, handeln.

Die Aufgabensteuerung, eine Komponente des Identity Manager-Servers, ist für den Lebenszyklus einer Aufgabe und der zugehörigen Ereignisse verantwortlich, wie in der folgenden Abbildung verdeutlicht:



Bei den meisten Ereignissen sind der Lebenszyklus, die Ausführung und die Aktionen unabhängig von anderen Ereignissen. (Bei Erstellungsaufgaben muss das Create-Ereignis des primären Objekts vor allen sekundären Ereignissen ausgeführt werden.)

In der Regel durchläuft ein Ereignis die folgenden Zustände:

- Start
- Ausstehend
- Bestätigt
- Ausführen
- Abgeschlossen
- Post

Hinweis: Identity Manager stellt Hooks, so genannte EventListeners, bereit, die zur Überwachung auf ein spezifisches Ereignis oder eine Gruppe von Ereignissen dienen. Wenn das Ereignis eintritt, führt der EventListener eine benutzerdefinierte Business-Logik aus, die auf das Ereignis und den aktuellen Ereigniszustand zugeschnitten ist. Mit Hilfe der EventListener-API können Sie benutzerdefinierte EventListener schreiben. Weitere Informationen hierzu finden Sie im *Programmierhandbuch für Java*.

Bilder für Admin-Aufgaben

Sie können Bilder erstellen, die Sie für Admin-Aufgaben verwenden, die Sie auf der Startseite platzieren.

Kapitel 4: Benutzer

Dieses Kapitel enthält folgende Themen:

Erstellen und Konfigurieren von Benutzern (siehe Seite 85)
Zulassen der Selbstregistrierung von Benutzern (siehe Seite 90)

Erstellen und Konfigurieren von Benutzern

Benutzerprofile erlauben Administratoren, Benutzerinformationen zu verwalten; Berechtigungen, Anwendungs- und Dienstzugriff zu verwalten; und Benutzerselbstverwaltung für ihre eigenen Konten und Dienste zu erteilen. Das Erstellen von Benutzerprofilen ist eine häufige Aufgabe für Systemadministratoren.

Wenn Sie einen Benutzer erstellen und konfigurieren, berücksichtigen Sie die folgenden Benutzerkontoelemente:

Self-Service Tasks: Benutzerkonten werden standardmäßig dafür konfiguriert, dem Benutzer Zugriff auf bestimmte Self-Service-Aufgaben zu erteilen, wie Kennwort- und Profilinformationen zu ändern. Ein Systemadministrator mit entsprechenden Berechtigungen kann ändern, welche Self-Service-Aufgaben einem Benutzer standardmäßig erteilt werden.

Gruppen: Gruppen vereinfachen die Rollenverwaltung. Zum Beispiel kann ein Systemadministrator mit entsprechenden Aufgaben mehrere Rollen konfigurieren, die das System automatisch einem Benutzer zuweist, der als Mitglied einer Gruppe hinzugefügt wird.

Admin-Rollen: Admin-Rollen definieren die Aufgaben, die ein Benutzer in der Benutzerkonsole ausführen kann. Zum Beispiel kann eine Aufgabe einem Benutzer erlauben, Benutzerkontoinformationen wie die Adresse oder die Berufsbezeichnung zu ändern. Eine andere Aufgabe kann einem Benutzer erlauben, Aufgaben zu verwalten, wie einem Benutzer die Mitgliedschaft in einer Gruppe zu erteilen. Wenn Sie einem Benutzer eine Admin-Rolle zuweisen, kann der Benutzer die der Rolle zugeordneten Aufgaben ausführen.

Endpunktkonten und Bereitstellungsrollen: Konten, die auf anderen Systemen vorhanden sind, werden Endpunktkonten genannt. Sie können Konten an Endpunkten CA CloudMinder-Benutzern durch Bereitstellungsrollen zuweisen. Zum Beispiel braucht ein Benutzer ein Exchange-Konto für E-Mail, ein Oracle-Konto für den Datenbankzugriff und ein Active Directory-Konto zur Verwendung eines Windows-Systems. Wenn Sie einem Benutzer eine Bereitstellungsrolle zuweisen, bekommt der Benutzer die Endpunktkonten, welche die Bereitstellungsrolle angibt.

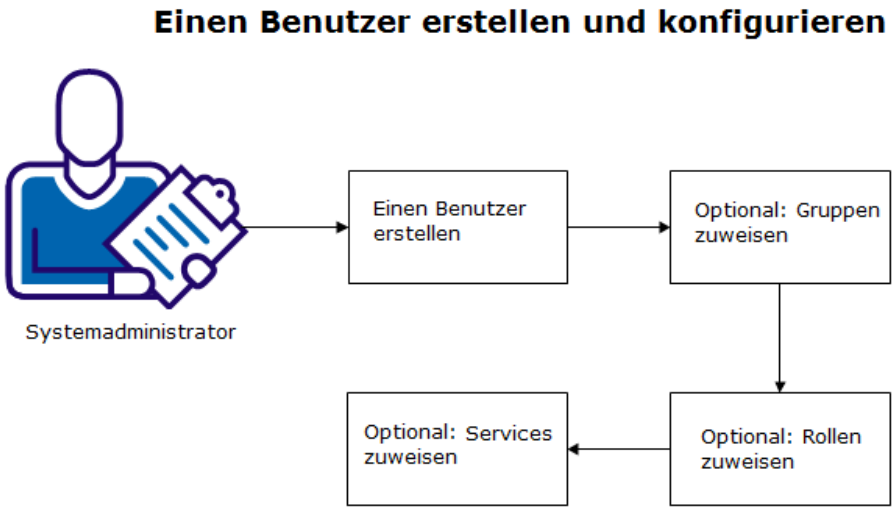
Zugriffsrollen: Zugriffsrollen bieten eine zusätzliche Möglichkeit, Berechtigungen in CA IdentityMinder oder einer anderen Anwendung anzugeben. Sie können Zugriffsrollen z. B. für Folgendes verwenden:

- Angeben von indirektem Zugriff auf ein Benutzerattribut
- Erstellen komplexer Ausdrücke
- Festlegen eines Attributs in einem Benutzerprofil, das von einer anderen Anwendung verwendet wird, um Berechtigungen zu bestimmen

Dienste: Dienste ermöglichen Ihnen, eine Auswahl von Anwenderaufgaben, Rollen, Gruppen und Attributen in einem einzigen Paket zu kombinieren. Sie können dieses Paket mit Berechtigungen als ein Set verwalten. Beispiel: Alle neuen Vertriebsmitarbeiter benötigen Zugriff auf eine definierte Aufgabengruppe, Konten auf speziellen Endpunktsystemen und spezifische Informationen, die ihren Benutzerkontenprofilen hinzugefügt wurden. Wenn Sie einen Dienst einem Benutzer zuweisen, empfängt der Benutzer den ganzen Satz Rollen, Aufgaben, Gruppen und Kontoattribute, die der Dienst angibt.

Kennwortrichtlinien: Mit Kennwortrichtlinien werden Benutzerkennwörter verwaltet, wobei Regeln und Einschränkungen im Hinblick auf Ablauf, Zusammensetzung und Verwendung von Kennwörtern erzwungen werden. Wenn ein Systemadministrator Kennwortrichtlinien für Ihre Umgebung erstellt hat, werden diese Richtlinien automatisch auf neue Benutzer übertragen, die einer oder mehren Kennwortrichtlinienregeln entsprechen. Ein Systemadministrator mit entsprechenden Aufgaben kann Kennwortrichtlinien ändern.

Das folgende Diagramm zeigt die erforderlichen Informationen und die durchzuführenden Schritte beim Erstellen und Konfigurieren eines Benutzers.



In den folgenden Themen wird das Erstellen und Konfigurieren von Benutzern ausführlich erklärt.

1. Erstellen eines Benutzers (siehe Seite 87)
2. Zuweisen von Gruppen (siehe Seite 88) (bei Bedarf)
3. Zuweisen einer Rolle zu einem Benutzer (siehe Seite 88) (bei Bedarf)
4. Zuweisen von Diensten (siehe Seite 89) (bei Bedarf)

Erstellen und Konfigurieren eines Benutzers

Verwenden Sie diesen Vorgang, um ein Benutzerprofil zu erstellen. Je nachdem, wie die Aufgabe "Benutzer erstellen" konfiguriert ist, können Sie diese Aufgabe auch verwenden, um zusätzliche Profilelemente zu definieren. Sie können einen Benutzer zu einer Gruppe hinzufügen oder den Benutzer zu einem Mitglied einer Admin- oder Bereitstellungsrolle machen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole als Benutzer mit Verwaltungsaufgaben an.

   Die Standardrolle "Benutzer-Manager" erteilt die entsprechenden Aufgaben.

2. Benutzer auswählen, Benutzer verwalten, Benutzer erstellen.

   Die Aufgabe "Benutzer erstellen" wird geöffnet.

3. Füllen Sie die Felder für die Benutzerprofilinformation nach Bedarf aus.
4. Klicken Sie auf "Weiter".
5. Vervollständigen Sie die Felder auf den anderen Registerkarten in der Aufgabe, falls zutreffend.

   Fügen Sie zum Beispiel den Benutzer einer Gruppe hinzu oder weisen Sie dem Benutzer eine Admin-Rolle, eine Bereitstellungsrolle oder einen Dienst zu, wenn diese Optionen verfügbar sind.
6. Klicken Sie auf "Fertig stellen".

   Der Benutzer wird erstellt.

Zuweisen einer Gruppe zu einem Benutzer

Sie können einen Benutzer zu einem Mitglied einer Gruppe machen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole als Benutzer mit Verwaltungsaufgaben an.

   Hinweis: Die Standardrolle "Benutzer-Manager" erteilt die entsprechenden Aufgaben. Ein Systemadministrator oder Mandantenadministrator (nur CA CloudMinder) verfügt in der Regel standardmäßig über diese Rolle.
2. Wählen Sie "Gruppen" und anschließend "Gruppenmitglieder ändern" aus.

   Eine Liste der Gruppen, die Sie verwalten können, wird angezeigt.
3. Wählen Sie eine Gruppe aus, und klicken Sie auf Auswählen.

   Eine Liste von Benutzern, die der Gruppe zugewiesen sind, wird angezeigt.
4. Klicken Sie auf "Benutzer hinzufügen".
5. Suchen Sie nach dem Benutzer, dem Sie die Gruppe zuweisen möchten.

   Um eine Liste aller Benutzer anzuzeigen, für die Sie Administratorrechte haben, klicken Sie auf "Suchen", ohne die Suchkriterien zu ändern.
6. Wählen Sie einen Benutzer aus, und klicken Sie auf Auswählen.

   Eine aktualisierte Liste von Benutzern, die der Gruppe zugewiesen sind, wird angezeigt.
7. Klicken Sie auf "Senden".

   Der angegebene Benutzer wird ein Mitglied der Gruppe.

Weisen Sie einen Service direkt einem Benutzer zu.

Sie können einem individuellen Benutzer Bereitstellungsrollen zuweisen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole als Benutzer mit der Aufgabe "Mitglieder/Administratoren von Bereitstellungsrolle ändern" an.
2. Wählen Sie die Option "Rollen und Aufgaben" aus.
3. Wählen Sie eine der folgenden Aufgaben aus:
   - Admin-Rollen, Mitglieder/Administratoren von Admin-Rolle ändern
   - Bereitstellungsrollen, Mitglieder/Administratoren von Bereitstellungsrolle ändern
   - Zugriffsrollen, Mitglieder/Administratoren von Zugriffsrolle ändern

   Ein Suchfenster wird geöffnet.
4. Wählen Sie die Rolle aus, die Sie dem Benutzer zuweisen möchten.

   Die Registerkarte "Mitgliedschaft" wird angezeigt.
5. Klicken Sie auf "Benutzer hinzufügen".
6. Suchen Sie nach dem Benutzer, dem Sie den Service zuweisen möchten.

   Um eine Liste aller Benutzer anzuzeigen, für die Sie Administratorrechte haben, klicken Sie auf "Suchen", ohne die Suchkriterien zu ändern.
7. Wählen Sie einen Benutzer aus, und klicken Sie auf "Auswählen".
8. Klicken Sie auf "Senden".

   Die angegebenen Rollen werden dem Benutzer zugewiesen.

Weisen Sie einen Service einem Benutzer zu.

Sie können einen Service direkt einem individuellen Benutzer zuweisen. Dieser Benutzer wird ein *Mitglied* des Services.

Gehen Sie wie folgt vor:

1. Wählen Sie im Navigationsmenü "Services" und "Zugriff anfordern und anzeigen".

   Eine Liste von Services, die Sie verwalten können, wird angezeigt.
2. Wählen Sie den Service aus, den Sie einem Benutzer zuweisen möchten, und klicken Sie auf "Auswählen".

   Eine Liste von Benutzern, die dem Service zugewiesen sind, wird angezeigt.
3. Klicken Sie auf "Zugriff anfordern".
4. Suchen Sie nach dem Benutzer, dem Sie den Service zuweisen möchten.

   Um eine Liste aller Benutzer anzuzeigen, für die Sie Administratorrechte haben, klicken Sie auf "Suchen", ohne die Suchkriterien zu ändern.

5. Wählen Sie einen Benutzer aus, und klicken Sie auf "Auswählen".

   Eine aktualisierte Liste von Benutzern, die dem Service zugewiesen sind, wird angezeigt.

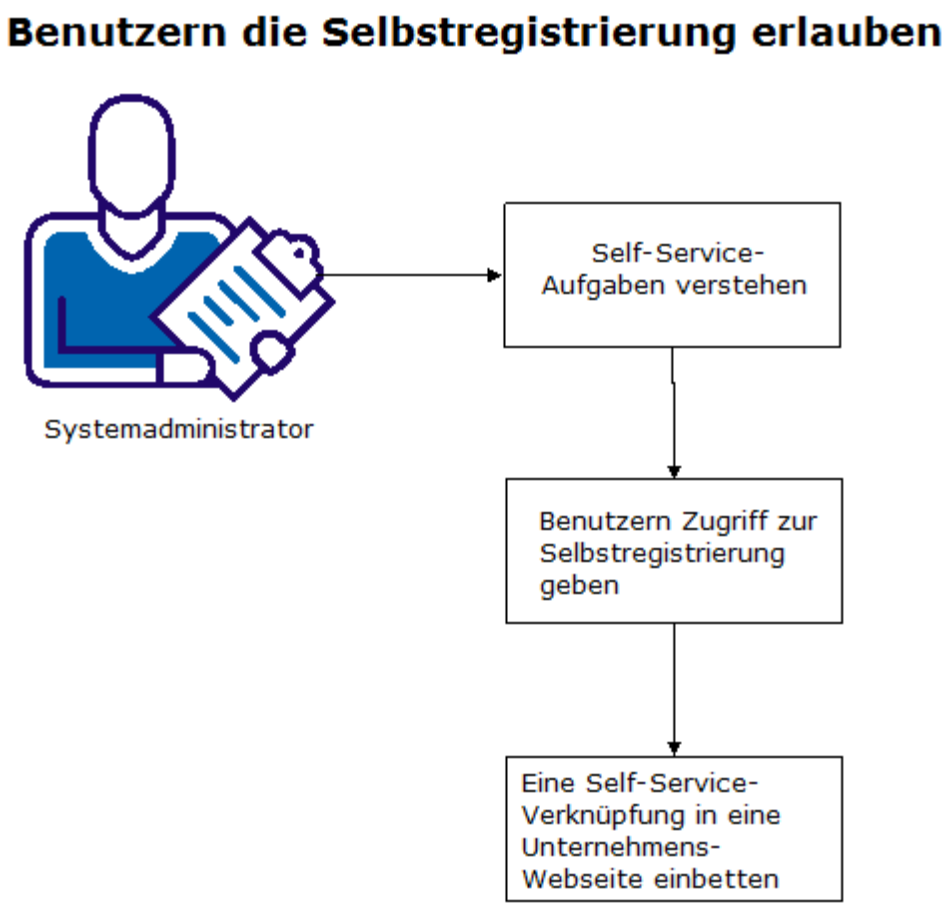
6. Klicken Sie auf "Änderungen speichern".

   Der angegebene Service wird für den Benutzer durchgeführt. Der Benutzer erhält alle im Service enthaltenen Anwendungen, Rollen, Gruppen und Attribute.

Zulassen der Selbstregistrierung von Benutzern

Self-Service-Aufgaben ermöglichen Benutzern, ihre eigene Umgebung zu verwalten. Die Selbstregistrierungs-Aufgabe erlaubt Benutzern, ihr eigenes Benutzerkonto und Profil von einer öffentlich verfügbaren Benutzerkonsole zu erstellen. Zum Beispiel erlaubt Bentley Cola neuen Mitarbeitern und Kunden, ihre eigenen Benutzerkonten und Profile über einen in die Bentley Cola-Unternehmens-Webseite eingebetteten Link zu erstellen.

Das folgende Diagramm zeigt die erforderlichen Informationen und die durchzuführenden Schritte zum Zulassen der Selbstregistrierung von Benutzern.



Die folgenden Themen enthalten Details, wie Benutzer Selbstregistrierungszugriff erhalten.

1. Wissenswertes über Self-Service-Aufgaben (siehe Seite 92)
2. Erteilen von Selbstregistrierungszugriff für Benutzer (siehe Seite 93)
3. Einbetten eines Self-Service-Links in eine Unternehmens-Website (siehe Seite 93)

Self-Service-Aufgaben

Self-Service-Aufgaben sind Aktionen, die Benutzer ausführen können, normalerweise über die Benutzerkonsole, um ihre eigenen Profile zu verwalten. Benutzerkonten werden standardmäßig dafür konfiguriert, dem Benutzer Zugriff auf bestimmte Self-Service-Aufgaben zu erteilen, wie Kennwort- und Profilinformationen zu ändern. Ein Systemadministrator mit entsprechenden Berechtigungen kann ändern, welche Self-Service-Aufgaben einem Benutzer standardmäßig erteilt werden.

Self-Service-Aufgaben sind in zwei Typen unterteilt:

- Öffentliche Aufgaben: Aufgaben, auf die Benutzer zugreifen können, ohne Anmeldeinformationen anzugeben. Beispiele für öffentliche Aufgaben sind die Aufgaben "Selbstregistrierung", "Kennwort vergessen" und "Benutzer-ID vergessen".
- Geschützte Aufgaben: Aufgaben, für die Benutzer gültige Anmeldeinformationen angeben. Beispiele umfassen Aufgaben zum Ändern von Kennwörtern oder Profilinformationen.

Die folgende Tabelle listet die standardmäßigen Self-Service-Aufgaben auf.

Aufgabentyp	Aufgaben
Öffentliche Aufgabe	■ Selbstregistrierung: Ermöglicht Benutzern, sich bei einer Unternehmens-Website zu registrieren ■ Kennwort vergessen: Zurücksetzen: Ermöglicht Benutzern, ein vergessenes Kennwort zurückzusetzen ■ Kennwort vergessen: Zeigt ein temporäres Kennwort an, das Benutzer zum Anmelden bei CA IdentityMinder verwenden können. Wenn sich der Benutzer anmeldet, wird er aufgefordert, ein neues Kennwort einzugeben ■ Benutzer-ID vergessen: Ruft eine vergessene Benutzer-ID ab oder setzt sie zurück
Geschützte Aufgabe	■ Zugriff anfordern und anzeigen: Erlaubt Benutzern, Zugriff auf Services und Entfernen von Services anzufordern. ■ Mein Kennwort ändern: Ermöglicht Benutzern, ihr Kennwort zurückzusetzen ■ Mein Profil ändern: Verwaltet Profilinformationen wie z. B Adresse und Telefonnummer ■ Meine Gruppen ändern: Ermöglicht Benutzern, Gruppen beizutreten ■ Meine Rollen anzeigen: Zeigt die Rollen eines Benutzers an ■ Meine übermittelten Aufgaben anzeigen: Zeigt CA IdentityMinder-Aufgaben an, die der Benutzer initiiert hat

Zugriff auf Self-Service-Aufgaben

Sobald Sie die Self-Service-Aufgaben für Ihre Umgebung konfiguriert haben, können Sie URLs für diese Aufgaben auf einer unternehmenseigenen Website hinzufügen.

URLs für Self-Service-Aufgaben haben das folgende Format:

https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=*task_tag*

wobei:

- *domain* dem voll qualifizierten Domänennamen des Webservers in der Umgebung entspricht, wo CA CloudMinder ausgeführt wird.
- *public_alias* dem öffentlichen Alias der Umgebung entspricht. Der Systemadministrator definiert den öffentlichen Alias, wenn die Umgebung erstellt wird.
- *task_tag* die eindeutige Kennung für die Aufgabe darstellt.

  Der Aufgaben-Tag für die Standardaufgabe "Kennwort vergessen: Zurücksetzen" lautet
  ForgottenPasswordReset.

  https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=ForgottenPasswordReset

  Der Aufgaben-Tag für die Standardaufgabe "Benutzer-ID vergessen" lautet ForgottenUserID:

  https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=ForgottenUserID

Einbetten eines Self-Service-Links in eine Unternehmens-Website

Um Zugriff auf eine öffentliche Self-Service-Aufgabe von einer Unternehmens-Website zu erlauben, können Sie einen Link zu einer Webseite hinzufügen. Wenn ein Benutzer auf den Link klickt, öffnet sich ein Aufgabenfenster. Wenn der Benutzer die Aufgabe abschließt, wird er standardmäßig an die Benutzerkonsole umgeleitet.

Um die Seite zu ändern, an die Benutzer umgeleitet werden, können Sie den Tag "task.RedirectURL" an die dem Link zugeordnete URL anhängen, wie folgt:

<A
href="http://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=*tasktag*&task.RedirectURL=http://*domain*/*redirect_URL*">*Link-Text*</A>

domain

Wobei Domain dem voll qualifizierten Domänennamen des Webservers in der Umgebung entspricht, wo CA IdentityMinder ausgeführt wird.

public_alias

Eine eindeutige Zeichenfolge, die zur URL für den Zugriff auf öffentliche Aufgaben hinzugefügt wird.

Öffentliche Aufgaben sind Self-Service-Aufgaben wie Selbstregistrierung oder vergessene Kennwortaufgaben. Benutzer müssen sich nicht anmelden, um auf öffentliche Aufgaben zuzugreifen.

Hinweis: Weitere Informationen zu öffentlichen Aufgaben und Aliasnamen finden Sie im *Konfigurationshandbuch*.

tasktag

Die eindeutige Kennung für die Aufgabe. Um den Aufgaben-Tag zu bestimmen, verwenden Sie "Admin-Aufgabe ändern", um das Profil für die Aufgabe anzuzeigen.

redirect_URL

Die URL, an die Benutzer weitergeleitet werden, nachdem sie die Aufgabe gesendet haben.

Zum Beispiel können Sie Benutzer an eine Willkommensseite umleiten, nachdem sie sich selbst registriert haben.

Link-Text

Der Text, auf den Benutzer klicken, um auf die Ziel-URL zuzugreifen.

Zum Beispiel kann ein Unternehmen einen Link hinzufügen, der Benutzern erlaubt, ein vergessenes Kennwort zurückzusetzen, und sie dann an eine Willkommensseite umleiten.

Im folgenden HTML sehen Sie ein Beispiel für Link-Text:

<A href="http://myserver.mycompany.org/iam/im/Employees/ui7/index.jsp?task.tag=ForgottenPasswordReset&task.RedirectURL=http://myserver.mycompany.org/ welcome.html">Mein Kennwort zurücksetzen</A>

Um Benutzer auf die Seite zurückzuleiten, von der aus sie auf die Self-Service-Aufgabe zugegriffen haben, geben Sie RefererURL als den Wert des Tags "task.RedirectURL" an, wie folgt:

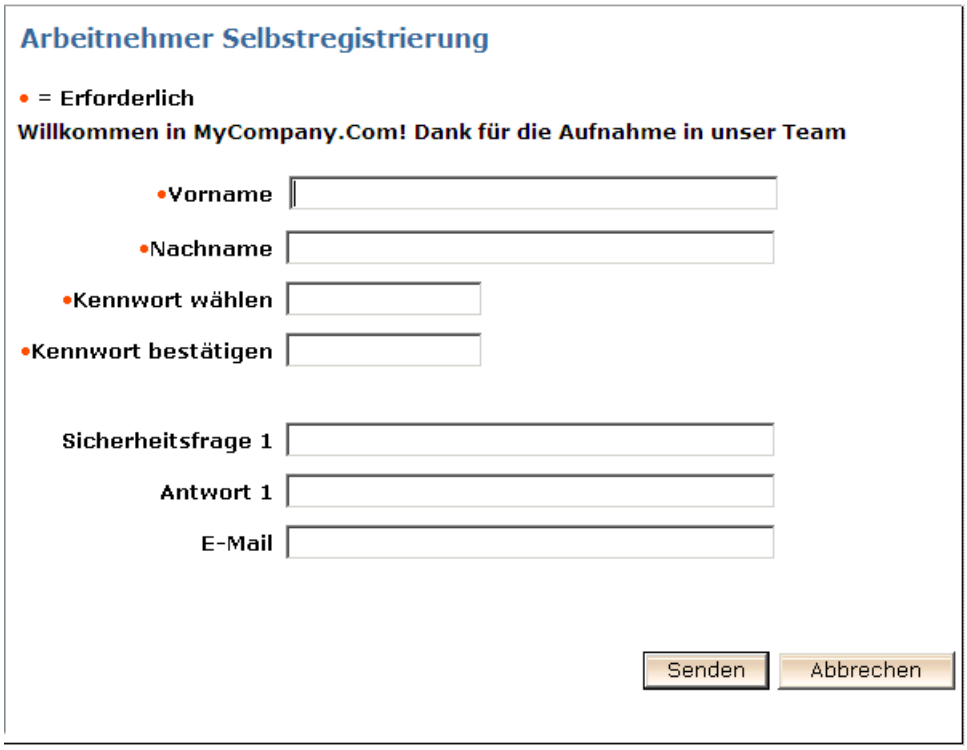
<A href="http://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=*tasktag*&task.RedirectURL=RefererURL</A>

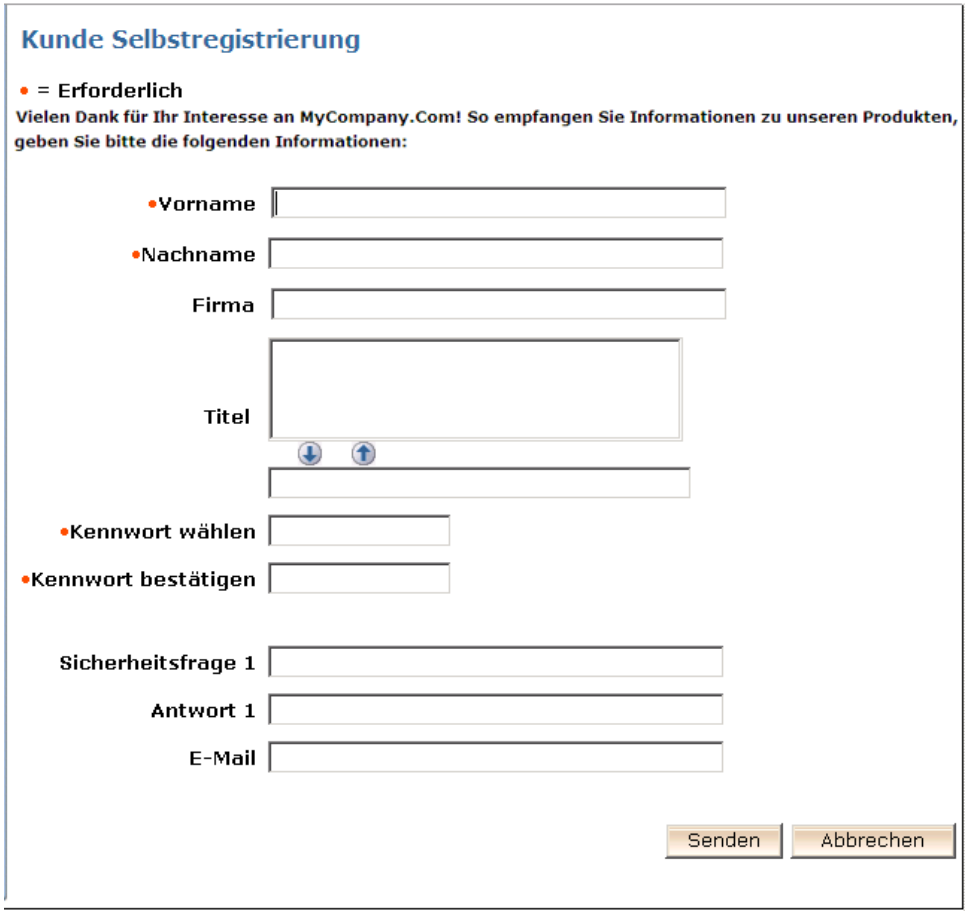
Mehrere Self-Service-Aufgaben konfigurieren

Sie können mehrere Self-Service-Aufgaben für unterschiedliche Benutzertypen erstellen. Sie können beispielsweise eine Aufgabe für das Registrieren neuer Arbeitnehmer und eine andere für das Registrieren neuer Kunden erstellen. Mit verschiedenen Selbstregistrierungsaufgaben können Sie die folgenden Aktionen durchführen:

- Verschiedene Informationen sammeln
- Benutzer in verschiedenen Organisationen registrieren
- Benutzer nach dem Registrieren auf verschiedene Abmeldeseiten weiterleiten
- Unterschiedliche Markenbildung verwenden

In den nachstehenden Abbildungen ist die Selbstregistrierungsaufgabe jeweils für neue Arbeitnehmer und neue Kunden dargestellt.





Wenn Sie mehrere Self-Service-Aufgaben desselben Typs konfigurieren möchten, geben Sie bei der Erstellung der Aufgabe einen einmaligen Tag an. Das Feld "Tag" befindet sich im Bildschirm "Profil konfigurieren" für die Aufgabe.

Wenn Sie einer Website den Link für den Zugriff auf die Aufgabe hinzufügen, wird der Aufgaben-Tag angehängt, wodurch eine eindeutige URL entsteht.

Sie können beispielsweise zwei Aufgaben folgendermaßen erstellen:

Aufgabe	Tag	URL
Als neuen Arbeitnehmer registrieren	selfregistration_employee	http://*domaene*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration_employee
Als Kunden registrieren	selfregistration_customer	http://*domaene*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration_customer

Einschränkung des Zugriffs auf die Rolle "Selbstverwaltung"

Standardmäßig wird die Rolle "Selbstverwaltung", durch die Benutzer ihre Profilinformationen verwalten sowie ihre Rollen und gesendete Aufgaben anzeigen dürfen, allen Benutzern zugewiesen.

Wenn Sie einer Teilmenge an Benutzern die Rolle "Selbstverwaltung" geben möchten, löschen Sie die bestehende Mitgliederrichtlinie und erstellen Sie eine neue Richtlinie, wie unter Definieren von Mitgliederrichtlinien für Admin-Rollen beschrieben.

Kapitel 5: Kennwort-Management

Dieses Kapitel enthält folgende Themen:

Kennwort-Management in Identity Manager (siehe Seite 99)
Kennwortrichtlinien – Übersicht (siehe Seite 100)
Erstellen von Kennwortrichtlinien (siehe Seite 101)
Kennwortrichtlinien verwalten (siehe Seite 115)
Kennwortrichtlinien und relationale Datenbanken (siehe Seite 115)
Kennwortkriterien für die CA IdentityMinder- und Siteminder-Integration (siehe Seite 115)
Zurücksetzen eines Kennworts oder Entsperren eines Kontos (siehe Seite 116)
Synchronisieren von Kennwörtern auf Endpunkten (siehe Seite 133)

Kennwort-Management in Identity Manager

Identity Manager enthält mehrere Funktionen zur Verwaltung von Benutzerkennwörtern:

- Kennwortrichtlinien: Mit diesem Richtlinien werden Benutzerkennwörter verwaltet, wobei Regeln und Einschränkung im Hinblick auf Ablauf, Zusammensetzung und Verwendung von Kennwörtern erzwungen werden.
- Kennwort-Manager: Administratoren, die die Rolle des Kennwort-Manager innehaben, können ein Kennwort zurücksetzen, wenn ein Benutzer den Helpdesk anruft.
- Self-Service-Kennwort-Management: Identity Manager enthält mehrere Self-Service-Aufgaben, mit denen der Benutzer sein eigenes Kennwort verwalten kann. Zu diesen Verwaltungsaufgaben gehören:
  - Selbstregistrierung: Der Benutzer gibt bei seiner Registrierung bei einer Firmen-Website ein Kennwort an.
  - Mein Kennwort ändern: Der Benutzer kann sein Kennwort ohne Hilfe von IT- oder Helpdesk-Arbeitnehmern ändern.
  - Kennwort vergessen: Der Benutzer kann ein vergessenes Kennwort zurücksetzen oder anfordern, nachdem Identity Manager seine Identität überprüft hat.
  - Kennwort zurücksetzen oder Konto entsperren (siehe Seite 116): Der Benutzer kann ein vergessenes Kennwort zurücksetzen bzw. abrufen oder auf einem System, auf dem er auf Identity Manager zugreift, ein Windows-Konto entsperren.
  - Benutzer-ID vergessen: Der Benutzer kann eine vergessene Benutzer-ID anfordern, nachdem Identity Manager seine Identität überprüft hat.

- Kennwortsynchronisierung in Endpunktkonten: Kennwortänderungen werden in Identity Manager sowie auf dem Bereitstellungsserver und seinen Zielsystemen synchronisiert. Neue Kennwörter werden gemäß den Kennwortrichtlinien in Identity Manager überprüft.

Kennwortrichtlinien – Übersicht

Eine Kennwortrichtlinie ist ein Satz von Regeln und Einschränkungen. Diese Regeln geben Kennworterstellung und Ablauf an. Wenn Sie eine Kennwortrichtlinie in einer CA IdentityMinder-Umgebung konfigurieren; gilt die Richtlinie für den mit dieser Umgebung verknüpften Benutzerspeicher. Wenn ein Benutzerverzeichnis mit mehreren Umgebungen verknüpft ist, kann die in einer Umgebung definierte Kennwortrichtlinie für andere Umgebungen gelten.

Bei einer Kennwortrichtlinie können Sie folgende Einstellungen konfigurieren:

Hinweis: Einige dieser Einstellungen erfordern Benutzerverzeichniszuordnungen für bestimmte Attribute. Siehe Aktivieren zusätzlicher Kennwortrichtlinien (siehe Seite 101).

- Anwenden von Kennwörtern auf einen bestimmten Satz von Benutzern
- Kennwortablauf: Definieren Sie Ereignisse, durch die ein Kennwort abläuft, z. B. das Verstreichen einer bestimmten Anzahl von Tagen oder eine bestimmte Anzahl von fehlgeschlagenen Anmeldeversuchen. Bei Ablauf eines Kennworts wird das Benutzerkonto deaktiviert.
- Zusammenstellung des Kennworts: Hier geben Sie an, aus welchen Komponenten neue Kennwörter bestehen müssen. Sie können die Einstellungen beispielsweise so konfigurieren, dass der Benutzer ein Kennwort erstellen muss, das mindestens acht Zeichen lang ist und eine Zahl und einen Buchstaben enthält.
- Reguläre Ausdrücke: Hier geben Sie einen Ausdruck an, der das Format eines gültigen Kennworts festlegt. Sie können angeben, ob Kennwörter mit diesem Format übereinstimmen oder nicht übereinstimmen. Sie können auch mehrere reguläre Ausdrücke angeben.
- Kennwortbeschränkungen: Legen Sie Beschränkungen für die Wiederverwendung von Kennwörtern fest, z. B. dass Benutzer 90 Tage warten müssen, bevor sie ein Kennwort wieder verwenden.
- Erweiterte Kennwortoptionen: Hier geben Sie Aktionen an, die CA IdentityMinder vor der Verarbeitung eines Kennworts durchführen soll, z. B. die Kleinschreibung von Kennwörtern. Sie können auch die Priorität einer Kennwortrichtlinie festlegen, sofern mehrere Kennwortrichtlinien gelten.

SiteMinder-Benutzer können Kennwortrichtlinien auch auf der SiteMinder Administrative-Benutzeroberfläche konfigurieren. Diese Richtlinien werden in der CA IdentityMinder-Benutzerkonsole angezeigt.

Hinweis: Wenn CA IdentityMinder in SiteMinder integriert ist, erzwingt SiteMinder *alle* Kennwortrichtlinien.

Erstellen von Kennwortrichtlinien

Sie erstellen Kennwortrichtlinien über die CA IdentityMinder-Benutzerkonsole.

Hinweis: Für die Verfügbarkeit einiger Kennwortrichtlinien-Optionen ist die Zuordnung bestimmter bekannter Attribute erforderlich. Siehe Aktivieren zusätzlicher Kennwortrichtlinien (siehe Seite 101).

Gehen Sie wie folgt vor:

1. Wählen Sie in der Benutzerkonsole "Richtlinien", "Kennwortrichtlinien verwalten", "Kennwortrichtlinie erstellen".
2. Geben Sie einen eindeutigen Namen sowie optional eine Beschreibung für die Kennwortrichtlinie ein.
3. Konfigurieren Sie die folgenden Kennwortrichtlinien-Einstellungen gemäß Ihrer Implementierung:
   - Kennwortrichtlinien auf einen Benutzersatz anwenden (siehe Seite 102)
   - Konfigurieren des Kennwortablaufs (siehe Seite 104)
   - Konfigurieren der Kennwortzusammenstellung (siehe Seite 107)
   - Angeben regulärer Ausdrücke (siehe Seite 109)
   - Festlegen von Kennwortbeschränkungen (siehe Seite 111)
   - Konfigurieren erweiterter Kennwortoptionen (siehe Seite 114)

Siehe Aktivieren zusätzlicher Kennwortrichtlinien.

Mit CA IdentityMinder können Sie grundlegende Kennwortrichtlinien erstellen, die Benutzerkennwörter durch das Erzwingen des Ablaufs, der Zusammenstellung und der Verwendung von Kennwörtern verwalten. Sie können auch die folgenden zusätzlichen Kennwortregeln und Beschränkungen definieren:

- Ablauf des Kennworts:
  - Fehlgeschlagene oder erfolgreiche Anmeldeversuche verfolgen
  - Anmeldung authentifizieren
  - Das Kennwort läuft ab, wenn es nicht geändert wird

- Kennwort-Inaktivität
- Ungültiges Kennwort
- Mehrere reguläre Ausdrücke

- Beschränkungen für Kennwort:
  - Mindestanzahl von Tagen vor Wiederverwendung
  - Mindestanzahl von Kennwörtern vor Wiederverwendung
  - Prozentualer Unterschied zum letzten Kennwort
  - Bei der Prüfung auf Unterschiede Sequenz ignorieren

Gehen Sie wie folgt vor:

1. Wechseln Sie in der Management-Konsole zu "Verzeichnisse", <Name des Verzeichnisses>, "Benutzer".
2. Überprüfen Sie, ob %PASSWORD DATA% und %ENABLED STATES% -> 'STATE' physischen Attributen zugeordnet sind.
3. Diese Attribute werden in den Beispieldateien "directory.xml" standardmäßig zugeordnet. Falls diese Attribute nicht zugeordnet sind, finden Sie entsprechende Informationen im *CA IdentityMinder-Konfigurationshandbuch*.

Kennwortrichtlinien auf einen Benutzersatz anwenden

Sie können Regeln angeben, die den Benutzersatz bestimmen, für den eine Kennwortrichtlinie gilt. Auf diese Weise kann es eine Kennwortrichtlinie für allgemeine Arbeitnehmer und eine weitere, strengere Richtlinie für Manager auf höchster Ebene geben.

Gehen Sie wie folgt vor:

1. Erstellen oder ändern Sie eine Kennwortrichtlinie in der Benutzerkonsole.
2. Wählen Sie den zu konfigurierenden Filtertyp im Feld "Verzeichnisfilter" aus.

   Eine Beschreibung zu den Filtertypen finden Sie in der nachstehenden Tabelle.

   Hinweis: Die Art des Benutzerspeichers, für den die Kennwortrichtlinie gilt, bestimmt die Optionen für das Listenfeld "Verzeichnisfilter". Einige Filtertypen sind für relationale Datenbanken und CA Directory-Benutzerspeicher nicht verfügbar, wenn CA IdentityMinder in SiteMinder integriert wird.
3. Legen Sie eine Bedingung fest, indem Sie ein Attribut und einen Operator auswählen und einen Wert eingeben.
4. Durch Klicken auf das Pluszeichen können Sie weitere Bedingungen hinzufügen.

Die nachstehende Tabelle enthält eine Beschreibung der Optionen für die Verzeichnisfiltertypen und Beispiele zu jedem Filtertyp. Attribute auf der linken Seite des "=" in den folgenden Beispielen entsprechen den Angaben im Benutzerverzeichnis-Definitionsbereich. Für Benutzeraufgaben des Typs "Erstellen" werden Kennwortrichtlinien mit konfigurierten Verzeichnisfiltern nur angewandt, wenn die beiden folgenden Bedingungen erfüllt sind:

- CA IdentityMinder ist nicht in SiteMinder integriert.
- Der Verzeichnisfiltertyp ist nicht "Benutzer", "Gruppe", "Gruppenfilter" oder "Gruppensuche".

Filtertyp	Verwendung.	Beispiel
In einer Organisation	Suchen und Auswählen einer Organisation.	
In einer Gruppe	Suchen und Auswählen einer Gruppe.	
Ein Benutzer	Suchen und Auswählen eines Einzelbenutzers.	
Benutzerfilter (Nicht verfügbar für relationale Datenbanken bei Integration mit SiteMinder)	Festlegen eines Filters für Benutzer	Arbeitnehmertyp = Auftragnehmer Abteilung = Sicherheit
Benutzersuchausdruck	Geben Sie eine Suchabfrage nach Benutzern ein.	uid=jsmith (für LDAP) TBLUSERS.ID = jsmith (für relationale Datenbanken)
Gruppenfilter (Nicht verfügbar für relationale Datenbanken bei Integration mit SiteMinder)	Legen Sie einen Filter für Gruppen fest.	Selbstabonnierend = *
Gruppensuchausdruck	Geben Sie eine Suchabfrage nach Gruppen ein.	cn=Sales (für LDAP) TBLGROUPS.NAME=GroupA (für relationale Datenbanken)
Organisationsfilter (Nicht verfügbar für relationale Datenbanken bei Integration mit SiteMinder)	Legen Sie einen Filter für Organisationen fest.	Name der Organisation = *Marketing

Filtertyp	Verwendung.	Beispiel
Organisationssuchausdruck	Geben Sie eine Suchabfrage nach Organisationen ein.	ou=Boston (für LDAP) TBLORGANIZATIONS.NAME=Boston (für relationale Datenbanken)
Suchen	Geben Sie eine Abfrage an, die in den anderen Optionen für den Filtertyp nicht enthalten ist.	(&(uid=*smith)(ou=Boston))

Konfigurieren des Kennwortablaufs

Um den Benutzerzugriff besser zu verwalten, können Sie Ereignisse wie mehrere fehlgeschlagene Anmeldeversuche oder Kontoinaktivität definieren. Wenn diese Ereignisse auftreten, deaktiviert CA IdentityMinder das verantwortliche Benutzerkonto. Wenn CA IdentityMinder mit SiteMinder integriert ist, können Sie eine Umleitung angeben.

Hinweis: Diese Einstellungen erfordern eine zusätzliche Konfiguration. Siehe Aktivieren zusätzlicher Kennwortrichtlinien (siehe Seite 101).

Sie können die folgenden Einstellungen für den Ablauf des Kennworts konfigurieren:

- Kontrollkästchen "Fehlgeschlagene/Erfolgreiche Anmeldeversuche verfolgen"
- Kontrollkästchen "Verfolgungsfehler: Authentifizierung beim Anmelden"
- Einstellungen für "Das Kennwort läuft ab, wenn es nicht geändert wird"
- Einstellungen für "Kennwort läuft aufgrund von Inaktivität ab"
- Einstellungen für "Ungültiges Kennwort"

Kontrollkästchen "Fehlgeschlagene/Erfolgreiche Anmeldeversuche verfolgen"

Dieses Kontrollkästchen aktiviert oder deaktiviert die Nachverfolgung von Benutzeranmeldeversuchen, einschließlich der Zeit des letzten Anmeldeversuchs. Wenn Sie dieses Kontrollkästchen aktivieren, schreibt CA IdentityMinder Anmeldeinformationen in ein Kennwortdatenattribut im Benutzerspeicher.

Hinweis: Diese Einstellung erfordert zusätzliche Konfiguration. Siehe Aktivieren zusätzlicher Kennwortrichtlinien (siehe Seite 101).

Wenn das Kontrollkästchen "Fehlgeschlagene Anmeldeversuche verfolgen" aktiviert ist, sind der Bereich "Ungültiges Kennwort" und das Kontrollkästchen "Verfolgungsfehler: Authentifizierung beim Anmelden" aktiv. Wenn das Kontrollkästchen "Erfolgreiche Anmeldeversuche verfolgen" aktiviert ist, sind der Bereich "Kennwort läuft aufgrund von Inaktivität ab" und das Kontrollkästchen "Verfolgungsfehler: Authentifizierung beim Anmelden" aktiv.

Wenn Sie mehrere Kennwortrichtlinien haben, stellen Sie sicher, dass alle anwendbaren Kennwortrichtlinien Anmeldungsdetails deaktivieren. Andernfalls kann eine einzelne Richtlinie, die die Nachverfolgung von Anmeldungsdetails aktiviert, falsches Verhalten der Kennwortrichtlinien verursachen.

Kontrollkästchen "Verfolgungsfehler: Authentifizierung beim Anmelden"

Das Aktivieren dieses Kontrollkästchens ermöglicht Anmeldungen, wenn die Benutzernachverfolgung fehlschlägt. Standardmäßig ist dieses Kontrollkästchen deaktiviert. Wenn Anmeldungsverfolgung deaktiviert ist, können sich Benutzer nicht anmelden.

Wenn Sie dieses Kontrollkästchen aktivieren, stellen Sie sicher, dass Sie auch das Kontrollkästchen "Fehlgeschlagene Anmeldeversuche verfolgen" oder das Kontrollkästchen "Erfolgreiche Anmeldeversuche verfolgen" auswählen.

Hinweis: Diese Einstellung erfordert zusätzliche Konfiguration. Siehe Aktivieren zusätzlicher Kennwortrichtlinien (siehe Seite 101).

Einstellungen für "Das Kennwort läuft ab, wenn es nicht geändert wird"

In den Feldern für "Das Kennwort läuft ab, wenn es nicht geändert wird" können Sie das Verhalten für Kennwörter konfigurieren, die abgelaufen sind. Optional können Sie angeben, wie weit im Voraus Benutzer gewarnt werden, dass ihr Kennwort bald abläuft.

Hinweis: Diese Einstellung erfordert zusätzliche Konfiguration. Siehe Aktivieren zusätzlicher Kennwortrichtlinien (siehe Seite 101).

Sie können die folgenden Felder konfigurieren:

Nach *<Anzahl>* Tagen

Bestimmt die Anzahl von Tagen, die CA IdentityMinder wartet, nachdem ein Kennwort abgelaufen ist, bevor der Benutzer deaktiviert wird oder eine Kennwortänderung erzwungen wird.

Hinweis: CA IdentityMinder deaktiviert das Benutzerkonto erst, wenn der Benutzer versucht, sich anzumelden, nachdem die angegebene Anzahl von Tagen abgelaufen ist.

Benutzer deaktivieren

Wenn Sie dieses Optionsfeld auswählen, wird der Benutzer deaktiviert, wenn das Kennwort abläuft. Deaktivierte Benutzer können wie folgt aktiviert werden:

- Über die Aufgabe "Benutzer aktivieren/deaktivieren" in der Benutzerkonsole. (Die Standardrollen für System-Manager, Organisations-Manager und Sicherheits-Manager umfassen die Aufgabe "Benutzer aktivieren/deaktivieren".)
- Über die Administratoroberfläche von SiteMinder.

  Hinweis: Weitere Informationen finden Sie im *Administrationshandbuch für SiteMinder-Richtlinienserver*.

Kennwortänderung erzwingen

Wenn Sie dieses Optionsfeld auswählen, wird die Kennwortänderung erzwungen, wenn der Benutzer das nächste Mal versucht, sich anzumelden.

Ablaufwarnungen senden für *<Anzahl>* Tage

Geben Sie die Anzahl von Tagen ein, wann ein Benutzer im Voraus benachrichtigt wird, dass sein Kennwort bald abläuft.

Einstellungen für "Kennwort läuft aufgrund von Inaktivität ab"

Mit den Einstellungen für "Kennwort läuft aufgrund von Inaktivität ab" können Sie die Zeit zwischen den Benutzeranmeldeversuchen angeben. Nach Ablauf dieser Zeit wird ein Benutzerkonto als inaktiv betrachtet. Sie können diesen Bereich auch verwenden, um eine Aktion anzugeben, wenn ein Benutzer, dessen Konto als inaktiv betrachtet wird, eine Anmeldungsberechtigung hat.

Um Einstellungen im Bereich "Kennwort läuft aufgrund von Inaktivität ab" zu konfigurieren, aktivieren Sie die Kontrollkästchen zur Nachverfolgung von Anmeldungsdetails.

Hinweis: Diese Einstellung erfordert zusätzliche Konfiguration. Siehe Aktivieren zusätzlicher Kennwortrichtlinien (siehe Seite 101).

Der Bereich "Kennwort läuft aufgrund von Inaktivität ab" enthält die folgenden Einstellungen:

- Nach *<Anzahl>* Tage – Bestimmt die Anzahl von Tagen mit Inaktivität, nach der ein Kennwort abläuft.
- Benutzer deaktivieren – Deaktiviert den Benutzer, wenn das Kennwort aufgrund von Inaktivität abläuft; das Benutzerkonto wird deaktiviert. Deaktivierte Benutzer müssen dann mithilfe der Aufgabe "Benutzer aktivieren/deaktivieren" wieder aktiviert werden.
- Kennwortänderung erzwingen – Erzwingt eine Kennwortänderung, wenn ein Kennwort aufgrund von Inaktivität abläuft. Der Benutzer ändert das Kennwort beim nächsten Anmeldeversuch.

Einstellungen für "Ungültiges Kennwort"

Im Bereich der Einstellungen für "Ungültiges Kennwort" können Sie angeben, wie viele fehlgeschlagene Anmeldungen erlaubt sind, bevor das Benutzerkonto deaktiviert wird. Sie können auch angeben, wie lange das Konto deaktiviert wird, bevor ein Benutzer versuchen kann, sich erneut anzumelden. Dieser Bereich ist nur verfügbar, wenn Sie das Kontrollkästchen "Fehlgeschlagene Anmeldeversuche verfolgen" aktiviert haben.

Hinweis: Diese Einstellung erfordert zusätzliche Konfiguration. Siehe Aktivieren zusätzlicher Kennwortrichtlinien (siehe Seite 101).

Der Bereich "Ungültiges Kennwort" enthält die folgenden Felder:

Konto deaktiviert nach *<Anzahl>* aufeinander folgende inkorrekte Kennwörter

Diese Einstellung bestimmt die Anzahl von aufeinander folgenden fehlgeschlagenen Anmeldeversuchen, die ein Benutzer vornehmen kann. Die Beschränkung der Anzahl von Fehlversuchen schützt vor Programmen, die dazu dienen, auf eine Ressource zuzugreifen, indem sie immer wieder Kennwörter ausprobieren, bis das richtige gefunden ist. Wenn ein Benutzer es nicht schafft, sich nach der angegebenen Anzahl von Versuchen korrekt anzumelden, deaktiviert CA IdentityMinder das Konto. Ein Administrator muss das Konto wieder aktivieren.

Nach *<Anzahl>* Minuten

Diese Einstellung bestimmt die Zeitdauer, die ein Benutzer wartet, bevor er einen weiteren Anmeldeversuch vornimmt oder sein Konto wieder aktiviert wird. Wenn der Benutzer ein anderes falsches Kennwort eingibt, deaktiviert CA IdentityMinder erneut das Konto. Der Benutzer wartet die angegebene Zeitdauer, bevor er es erneut versucht.

Einen Anmeldeversuch erlauben

Diese Einstellung gibt die Anzahl von Minuten an, nachdem ein Benutzer ein falsches Kennwort eingibt, bevor ein zusätzlicher Anmeldeversuch möglich ist.

Konto wieder aktivieren

Diese Einstellung aktiviert ein Konto wieder nach der angegebenen Zahl von Minuten.

Konfigurieren der Kennwortzusammenstellung

Sie können Regeln angeben, die die Zeichenzusammenstellung von neu erstellten Kennwörtern bestimmen. Beachten Sie die maximale Kennwortlänge, wenn Sie Werte für Zeichenanforderungen bestimmen. Wenn die Gesamtzahl der Buchstaben und Ziffern die maximale Kennwortlänge überschreitet, werden alle Kennwörter abgelehnt. Wenn zum Beispiel "Buchstaben oder Ziffern" jeweils auf sechs festgelegt sind, enthalten alle Kennwörter mindestens 12 Zeichen (6 Buchstaben und 6 Ziffern). In diesem Beispiel werden - wenn eine maximale Kennwortlänge acht Zeichen ist - alle Kennwörter abgelehnt.

Zu den Kennwortzusammenstellungs-Einstellungen gehören folgende:

Minimale Kennwortlänge

Gibt eine Minimallänge für Benutzerkennwörter an.

Maximale Kennwortlänge

Gibt die größtmögliche Länge für Benutzerkennwörter an.

Maximale Anzahl wiederholter Zeichen

Bestimmt die Höchstanzahl von identischen Zeichen, die fortlaufend in einem Kennwort angezeigt werden können.

Wenn dieser Wert beispielsweise auf 3 festgelegt wird, kann "aaaa" nirgends im Kennwort vorkommen. Allerdings ist "aaa" innerhalb eines Kennworts annehmbar. Legen Sie diesen Wert fest, um sicherzustellen, dass Benutzer keine Kennwörter aus einem einzelnen Zeichen eingeben können.

Großbuchstaben

Gibt an, ob Großbuchstaben erlaubt sind, und ggf. die minimale Anzahl, die ein Kennwort enthalten muss.

Kleinbuchstaben

Gibt an, ob Kleinbuchstaben erlaubt sind, und ggf. die minimale Anzahl, die ein Kennwort enthalten muss.

Buchstaben

Gibt an, ob Buchstaben erlaubt sind, und ggf. die minimale Anzahl, die ein Kennwort enthalten muss.

Hinweis: Das Kontrollkästchen "Buchstaben" wird automatisch aktiviert, wenn Sie Großbuchstaben oder Kleinbuchstaben zulassen.

Ziffern

Gibt an, ob Zahlen erlaubt sind, und ggf. die minimale Anzahl, die ein Kennwort enthalten muss.

Buchstaben und Ziffern

Gibt an, ob Buchstaben und Ziffern erlaubt sind, und ggf. die minimale Anzahl, die ein Kennwort enthalten muss. Wenn diese Einstellung zusammen mit "Ziffern" festgelegt wird, können Zeichen beide Anforderungen erfüllen. Zum Beispiel wenn diese Einstellung und "Ziffern" auf 4 festgelegt werden, ist das Kennwort "1234" ein gültiges Kennwort.

Hinweis: Das Kontrollkästchen "Buchstaben und Ziffern" wird automatisch aktiviert, wenn Sie Großbuchstaben, Kleinbuchstaben oder Zahlen zulassen.

Satzzeichen

Gibt an, ob Großbuchstaben erlaubt sind, und ggf. die minimale Anzahl, die ein Kennwort enthalten muss. Satzzeichen können Punkte, Kommas, Ausrufezeichen, Schrägstriche, Gedankenstriche und Bindestriche sein.

Nicht (be-)druckbar

Gibt an, ob nicht druckbare Zeichen erlaubt sind, und ggf. die minimale Anzahl, die ein Kennwort enthalten kann. Diese Zeichen können auf einem Computerbildschirm nicht angezeigt werden.

Hinweis: Bestimmte Browser unterstützen nicht druckbare Zeichen nicht.

Nicht-alphanumerisch

Gibt an, ob nicht alphanumerische Zeichen wie Satzzeichen und andere Symbole ("@", "$" und "*") erlaubt sind, und ggf. die minimale Anzahl, die ein Kennwort enthalten kann. Nicht druckbare Zeichen sind ebenfalls eingeschlossen. Ein nicht alphanumerisches Zeichen erfüllt ebenfalls die Zeichenanforderungen von Satzzeichen und nicht druckbaren Zeichen.

Angeben regulärer Ausdrücke

Reguläre Kennwortausdrücke lassen Sie reguläre Ausdrucks-Textmuster für Zeichenfolgenübereinstimmung angeben, mit der jedes Kennwort übereinstimmen bzw. nicht übereinstimmen muss, um gültig zu sein. Dieser Test kann nützlich sein, wenn Sie zum Beispiel festlegen wollen, dass das erste Zeichen eine Ziffer ist und das letzte Zeichen keine ist.

Sie konfigurieren mehrere Ausdrücke für eine einzelne Kennwortrichtlinie. Wenn Sie mehrere Ausdrücke erstellen, stimmen zulässige Kennwörter mit *allen* angegebenen Ausdrücken überein.

Gehen Sie wie folgt vor:

1. Geben Sie einen beschreibenden Tag für den Ausdruck (keine Leerzeichen) in das Namensfeld ein.
2. Geben Sie einen regulären Ausdruck unter Verwendung der in der Syntax für reguläre Ausdrücke beschriebenen Syntax in das Feld "Müssen übereinstimmen" ein.
3. Wenn das Kennwort nicht mit dem regulären Ausdruck übereinstimmen soll, aktivieren Sie das Kontrollkästchen in der Spalte "Darf NICHT übereinstimmen".

Hinweis: Sie können mehrere Ausdrücke angeben, indem Sie auf das Pluszeichen (+) klicken, um den Ausdruck hinzuzufügen.

Beispiel: Die folgende reguläre Ausdrucksdefinition kann verwendet werden, um zu erzwingen, dass alle Kennwörter mit einem Groß- oder Kleinbuchstaben anfangen:
Name: MustStartAlpha

Expression: [a-zA-Z].*

Syntax regulärer Ausdrücke

Dieser Abschnitt beschreibt die Syntax, mit der Sie reguläre Ausdrücke für die Kennwortübereinstimmung erstellen. Diese Syntax ist konsistent mit der Syntax regulärer Ausdrücke, die für Ressourcenübereinstimmung unterstützt wird, wenn Bereiche angegeben werden.

Zeichen	Ergebnisse
\	Wird als Escape-Zeichen für ein Metazeichen (wie '*') verwendet
\\	Stimmt mit einem einzelnen '\'-Charakter überein
(A)	Gruppiert Unterausdrücke (wirkt sich auf die Reihenfolge der Musterauswertung aus)
[abc]	Einfache Zeichenklasse (jedes Zeichen innerhalb der Klammern stimmt mit dem Zielzeichen überein)
[a-zA-Z]	Zeichenklasse mit Bereichen (jeder Zeichenbereich innerhalb der Klammern stimmt mit dem Zielzeichen überein)
[^abc]	Negierte Zeichenklasse
.	Stimmt mit jedem Zeichen außer 'neue Zeile' überein
^	Übereinstimmungen nur am Anfang einer Zeile
$	Übereinstimmungen nur am Ende einer Zeile
A*	Stimmt mit 0 oder mehr A überein ("gierig")
A+	Stimmt mit 1 oder mehr A überein ("gierig")
A?	Stimmt mit 1 oder 0 A überein ("gierig")
A*?	Stimmt mit 0 oder mehr A überein ("zurückhaltend")
A+?	Stimmt mit 1 oder mehr A überein ("zurückhaltend")
A??	Stimmt mit 0 oder 1 A überein ("zurückhaltend")
AB	Stimmt mit A gefolgt von B überein
A|B	Stimmt mit A oder B überein
\1	Rückverweis auf den 1. eingeklammerten Unterausdruck
n	Rückverweis auf den *n*. eingeklammerten Unterausdruck

Alle Abschlussoperatoren (+, *, ?) sind standardmäßig "gierig". Das bedeutet, dass sie mit so vielen Elementen der Zeichenfolge wie möglich übereinstimmen, ohne die gesamte Übereinstimmung zu verhindern. Wenn Sie möchten, dass ein Abschluss "zurückhaltend" ist (nicht "gierig"), können Sie einfach ein ’?’ anfügen. Ein zurückhaltender Abschluss stimmt bei der Suche nach Übereinstimmungen mit so wenigen Elementen der Zeichenfolge wie möglich überein.

Festlegen von Kennwortbeschränkungen

Sie können die Verwendung von Kennwörtern einschränken. Die Einschränkungen schließen ein, wie lange ein Benutzer warten muss, bevor er ein Kennwort wieder benutzen kann, und wie unterschiedlich das Kennwort gegenüber einem früher ausgewählten sein muss. Sie können auch Benutzer davon abhalten, Wörter anzugeben, die Sie als Sicherheitsrisiko einstufen oder die persönliche Daten enthalten.

Hinweis: Diese Einstellung erfordert zusätzliche Konfiguration. Siehe Aktivieren zusätzlicher Kennwortrichtlinien (siehe Seite 101).

Der Bereich "Einschränkung" umfasst die folgenden Felder:

Mindestanzahl von Tagen vor Wiederverwendung

Legt fest, wie viele Tage ein Benutzer warten muss, bevor er ein Kennwort wieder verwenden darf.

Mindestanzahl von Kennwörtern vor Wiederverwendung

Legt fest, wie viele Kennwörter verwendet werden müssen, bevor ein Kennwort wieder verwendet werden kann.

Hinweis: Wenn Sie eine Zeitdauer und die Anzahl von Kennwörtern angeben, werden beide Kriterien erfüllt, bevor ein Kennwort wieder verwendet werden kann. Zum Beispiel können Sie eine Kennwortrichtlinie konfigurieren, die erfordert, dass Benutzer 365 Tage warten und 12 Kennwörter angeben, bevor sie ein Kennwort wieder verwenden dürfen. Wenn nach einem Jahr nur sechs Kennwörter verwendet wurden, müssen weitere sechs verwendet werden, bevor der Benutzer das erste Kennwort wieder einsetzen kann.

Prozentualer Unterschied zum letzten Kennwort

Gibt den Prozentsatz an Zeichen an, die ein neues Kennwort enthalten muss. Sie können den Wert auf 100 festlegen. In diesem Fall darf das neue Kennwort keine Zeichen enthalten, die im früheren Kennwort enthalten waren.

Bei der Prüfung auf Unterschiede Sequenz ignorieren

Ignoriert die Position der Zeichen im Kennwort, wenn der Prozentsatz bestimmt wird.

Zum Beispiel ist bei dem anfänglichen Kennwort BASEBALL12 und aktiviertem Kontrollkästchen "Bei der Prüfung auf Unterschiede Sequenz ignorieren" 12BASEBALL nicht zulässig. Bei deaktiviertem Kontrollkästchen ist 12BASEBALL ein zulässiges Kennwort, weil jeder Buchstabe in einer unterschiedlichen Position auftritt.

Für erhöhte Sicherheit sollten Sie das Kontrollkästchen "Bei der Prüfung auf Unterschiede Sequenz ignorieren" aktivieren.

Kennwörter	Prozentuale Abweichung	Sequenz ignorieren	Akzeptiert
BASEBALL12 (Alt)	0	Aktiviert	Y
12BASEBALL		Deaktiviert	Y
BASEBALL12 (Alt)	100	Aktiviert	N
12BASEBALL		Deaktiviert	Y
BASEBALL12 (Alt)	0	Aktiviert	Y
12SOFTBALL		Deaktiviert	Y
BASEBALL12 (Alt)	90	Aktiviert	N
12SOFTBALL		Deaktiviert	Y
BASEBALL12 (Alt)	100	Aktiviert	N
12SOFTBALL		Deaktiviert	N

Profilattribute

Wenn Sie das Feld "Übereinstimmungslänge" konfigurieren, werden Benutzer daran gehindert, persönliche Daten in ihren Kennwörtern zu verwenden. Das Feld "Übereinstimmungslänge" bestimmt die minimale Sequenzlänge, die die Kennwortrichtlinie mit Attributen im Verzeichniseintrag vergleicht. Wenn dieser Wert beispielsweise auf vier festgelegt wird, überprüft CA IdentityMinder, dass das Kennwort nicht die letzten vier Zeichen der Benutzerprofilattribute einschließt, zum Beispiel Nachname oder Telefonnummer.

Wörterbuch

Gibt eine Liste von Zeichenfolgen an, die nicht in Kennwörtern verwendet werden können.

Hinweis: Auf die Schlusszeile der Wörterbucheingabe folgt ein Absatzende.

Die Wörterbucheinstellungen enthalten die folgenden Felder:

- Pfad – Enthält den vollständigen Pfad und den Namen der Wörterbuchdatei.
- Übereinstimmungslänge – Steuert die Länge von Zeichenfolgen, die mit Werten in der Wörterbuchdatei verglichen werden. Der Vergleich ignoriert die Groß-/Kleinschreibung der Zeichenfolgen. Sie können das Feld "Übereinstimmungslänge" leer lassen oder auf null festlegen. In diesen Fällen lehnt CA IdentityMinder nur Kennwörter ab, die mit einer Zeichenfolge im Wörterbuch genau übereinstimmen. Wenn die Übereinstimmungslänge größer ist als null, lehnt CA IdentityMinder unter den folgenden Bedingungen Eingaben ab:
  - Das Kennwort schließt eine Teilzeichenfolge ein, die mit der gleichen Buchstabenfolge wie ein Wörterbucheintrag anfängt.
  - Die Anzahl von aufeinander folgenden übereinstimmenden Zeichen ist größer als oder gleich der im Feld "Übereinstimmungslänge" angegebenen Zahl.

  Nehmen Sie zum Beispiel eine Wörterbuchdatei, die die folgenden Eingaben enthält:
  - Löwe
  - Tiger
  - Bär

  Wenn das Feld "Übereinstimmungslänge" auf vier festgelegt wird, ergeben sich folgende Aktionen:

  "Teddybär" wird abgelehnt, weil "bär" mit dem Eintrag "Bär" in der Wörterbuchdatei übereinstimmt.

  "Prestige" wird abgelehnt, weil "tige" mit den ersten vier Buchstaben des Eintrags "Tiger" in der Wörterbuchdatei übereinstimmt.

  "Geigerzähler" wird akzeptiert, da "iger" nicht den Anfangsbuchstaben des Eintrags "Tiger" in der Wörterbuchdatei einschließt.

Konfigurieren erweiterter Kennwortoptionen

Mit erweiterten Kennwortrichtlinien-Optionen können Sie die Vorverarbeitung von gesendeten Kennwörtern vor der Validierung und Speicherung konfigurieren. Sie können der Richtlinie auch eine Priorität zuweisen, um eine voraussagbare Auswertung von mehreren Kennwortrichtlinien zu ermöglichen, die sich auf dasselbe Benutzerverzeichnis oder denselben Namespace beziehen.

Groß-/Kleinschreibung nicht erzwingen | Großschreibung erzwingen | Kleinschreibung erzwingen

Entscheiden Sie, ob vor der Verarbeitung und Speicherung von Kennwörtern deren Groß- oder Kleinschreibung erzwungen wird. Wählen Sie eine Option zur Erzwingung der Groß-/Kleinschreibung, indem Sie auf das Optionsfeld "Großschreibung erzwingen" bzw. "Kleinschreibung erzwingen" klicken. Stellen Sie ansonsten sicher, dass das Optionsfeld "Groß-/Kleinschreibung nicht erzwingen" (Standard) aktiviert ist.

Wichtig! Stellen Sie sicher, dass jede Option zur Erzwingung der Groß-/Kleinschreibung, die Sie angeben, konsistent mit den von Ihnen definierten Zusammenstellungsanforderungen bezüglich Groß-/Kleinschreibung ist.

Führende Leerzeichen entfernen

Wählen Sie dies aus, um vor der Verarbeitung führende Leerzeichen aus Kennwörtern zu entfernen.

Nachgestellte Leerzeichen entfernen

Wählen Sie dies aus, um vor der Verarbeitung führende Leerzeichen aus Kennwörtern zu entfernen.

Eingebettete Leerzeichen entfernen

Wählen Sie dies aus, um vor der Verarbeitung alle eingebetteten Leerzeichen zu entfernen.

Hinweis: Einige Benutzerverzeichnisimplementierungen entfernen automatisch führende oder nachgestellte Leerzeichen aus Attributwerten (in denen Benutzerkennwörter gespeichert werden), bevor sie gespeichert werden. Die Einstellungen, die Sie in Ihrer Kennwortrichtlinie angeben, haben keine Auswirkung.

Auswertungspriorität

Gibt die Auswertungspriorität für die Kennwortrichtlinie an. Der Wert liegt im Bereich 0 (der Standard) bis 999. Anwendbare Richtlinien werden in absteigender Reihenfolge ausgewertet (999 zuerst; 0 zuletzt).

Kennwortrichtlinien mit niedrigerer Priorität übernehmen

Bestimmt, ob Kennwortrichtlinien geringerer Priorität nach dieser angewandt werden.

Kennwortrichtlinien verwalten

Administratoren mit den entsprechenden Berechtigungen können die Kennwortrichtlinien mit den Aufgaben zum Anzeigen, Ändern, Erstellen und Löschen von Kennwortrichtlinien verwalten. Diese Aufgaben werden standardmäßig in der Kategorie "Richtlinien" angezeigt.

Wenn Sie auf eine dieser Aufgaben zugreifen, zeigt CA IdentityMinder eine Liste der Kennwortrichtlinien an, die für den mit der aktuellen CA IdentityMinder-Umgebung verknüpften Benutzerspeicher gelten. Wenn CA IdentityMinder in SiteMinder integriert ist, enthält die Liste möglicherweise auch Kennwortrichtlinien, die mithilfe der Kennwortservices auf der SiteMinder Administrative-Benutzeroberfläche erstellt wurden. Sie können sowohl in CA IdentityMinder als auch in SiteMinder erstellte Kennwortrichtlinien verwalten.

Kennwortrichtlinien und relationale Datenbanken

Wenn Sie eine Kennwortrichtlinie konfigurieren, die für eine relationale Datenbank gilt, müssen Sie das Kennwortdatenattribut für das SiteMinder-Benutzerverzeichnis im folgenden Format konfigurieren:

Tabellenname.Spaltenname

Zur Vermeidung von Syntaxproblemen bei der Ausführung sollte sich dieses Feld in der Haupttabelle befinden.

Kennwortkriterien für die CA IdentityMinder- und Siteminder-Integration

Wenn CA IdentityMinder in SiteMinder integriert ist und die Kennwortverarbeitungsfunktion von Siteminder verwendet, werden Kennwortrichtlinien vom Siteminder-Richtlinienspeicher übernommen. Erstellen Sie in diesem Fall Kennwörter, die den Kennwortkriterien von Siteminder entsprechen. Die folgenden Interpunktionszeichen sind die einzigen Interpunktionszeichen, die den Siteminder-Kennwortkriterien entsprechen:

'*', '(', '\',',','@','"',':','#','_','-','!','&','?',')','(','{','}','*','.','/' “

Wichtig: CA IdentityMinder erhebt keine Beschränkung der Verwendung von Interpunktionszeichen in Kennwörtern. Wenn Sie beabsichtigen, die Siteminder-Kennwortfunktion zu verwenden, empfehlen wir allerdings, dass Sie Kennwörter errichten, die den Siteminder-Beschränkungen entsprechen.

Zurücksetzen eines Kennworts oder Entsperren eines Kontos

Wenn Benutzer ihre Kennwörter auf Windows-Systemen vergessen, können Sie Self-Service konfigurieren, um dem Benutzer eine Eingabeaufforderung auf dem Windows-Anmeldebildschirm anzuzeigen. Sie können diese Funktion verwenden, indem Sie einer dieser Komponenten installieren:

- Die GINA-Komponente (GINA - Graphical Identification and Authorization) für Windows 2000, 2003 und Windows XP
- Der "Credential Provider" für Windows Vista und Windows 7

Mit dieser Funktion wird der Benutzer in Self-Service über den Cube-Webbrowser angemeldet, wo eine Seite zur Anfrage einer Kennwortänderung angezeigt wird. Nachdem diese Seite ausgefüllt wird, klickt der Benutzer auf "Zurückkehren", um zum Windows-Anmeldebildschirm zurückzukehren.

Installieren von GINA oder Credential Provider

Sie können GINA (für Windows 2000, 2003 und XP) oder Credential Provider (für Windows Vista oder 2008) auf einem Windows-System installieren, von dem aus ein Benutzer auf eine Identity Manager-Umgebung zugreift.

So installieren Sie GINA oder Credential Provider:

1. Suchen Sie die heruntergeladenen CA IdentityMinder-Bereitstellungskomponenten oder andere Installationsmedien.
2. Rufen Sie das Installationsprogramm aus dem Ordner \Agent auf.

   Hinweis: Wenn Sie Credential Provider auf einem 64-Bit-Betriebssystem installieren, wählen Sie die 64-Bit-Version dieser Software.
3. Befolgen Sie die Aufforderungen des Assistenten, um die Fragen zu beantworten.
4. Nach der Installation der Komponente konfigurieren Sie sie mit Hilfe des geeigneten Verfahrens:
   - Konfigurieren von GINA (siehe Seite 117)
   - Konfigurieren des Credential Providers

Konfigurieren von GINA

Mit dem Tool für die Konfiguration von GINA können Sie die GINA-Standardwerte bearbeiten und zum erneuten Verpacken in eine Registrierungsdatei (.reg-Datei) exportieren. Die Einstellungen können auch auf dem aktuellen System angewendet werden.

So konfigurieren Sie GINA:

1. Wechseln Sie im Windows Explorer in den Ordner, in dem GINA installiert wurde. Beispiel:

   ```
   C:\Programme\CA\Identity Manager\Bereitstellungs-GINA
   ```

2. Doppelklicken Sie auf die folgende ausführbare Datei:

   ```
   ginaconfig.exe
   ```

3. Geben Sie in die Felder für die GINA-Einstellungen die folgenden Informationen ein:

   Link1-Befehl

   Die vollständige Befehlszeile, die ausgeführt werden soll, wenn der Benutzer auf den Link "Kennwort vergessen" klickt. Dieser Link sollte eine URL zu einer Webschnittstelle zum Zurücksetzen von Kennwörtern laden. Beispiel für einen Befehl:

   ```
   http://eastern.local:8080/iam/im/pub/ca/index.jsp?task.tag=ForgottenPassword
   ```

   Für diese URL muss die Selbstregistrierung in der Umgebung funktionieren. Stellen Sie außerdem sicher, dass die Self-Service-URL für die CA IdentityMinder-Umgebung auf dem System funktioniert, auf dem Sie GINA installieren.

   Link2-Befehl

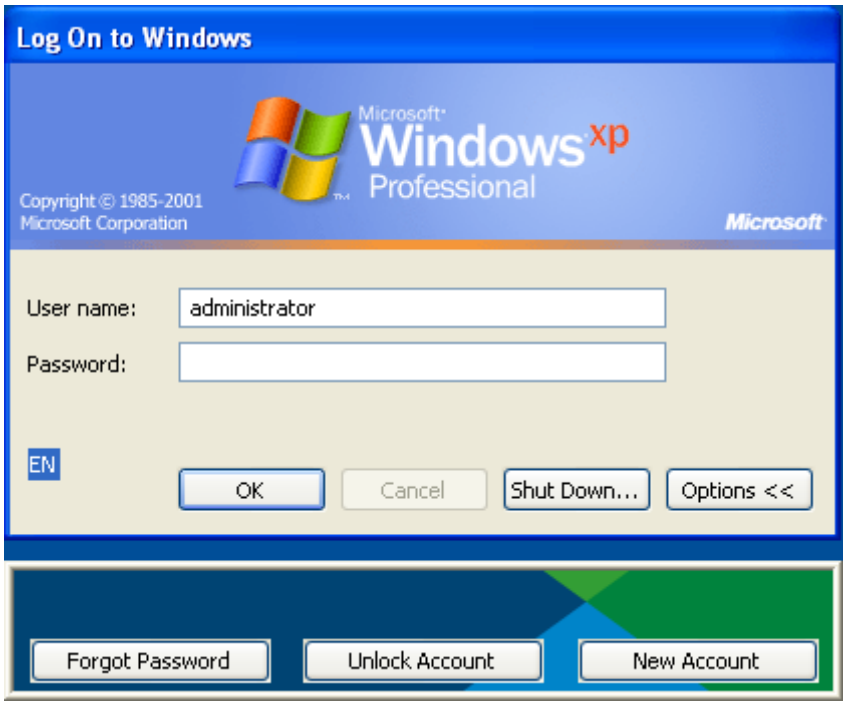
   Die vollständige Befehlszeile, die ausgeführt werden soll, wenn der Benutzer auf den Link "Konto entsperren" klickt. Dieser Link sollte eine URL zu einer Webschnittstelle laden, über die der Benutzer ein Konto entsperren kann.

   Link3-Befehl

   Die vollständige Befehlszeile, die ausgeführt werden soll, wenn der Benutzer auf den Link für ein neues Konto klickt. Dieser Link sollte eine URL zu einer Webschnittstelle laden, über die der Benutzer ein Konto erstellen kann.

   Verwenden eines unverankerten Dialogfelds

   Eine Alternative zu den Link-Befehlen, die dieselben Funktionen bietet und während der Anmeldung bei Windows angezeigt wird. Dieses Dialogfeld kann auch ein BMP-, WMF- oder ICO-Bild im Hintergrund rendern. Nachfolgend sehen Sie ein Beispiel für ein unverankertes Dialogfeld:



Domäne

Name der Bereitstellungsdomäne.

Section 508 Compliance (Use Return in menu) - Konformität mit Abschnitt 508 (Rückgabefunktion im Menü verwenden)

Aktiviert die Rückgabefunktion in einem Menü. Wenn diese Option nicht ausgewählt ist, wird das Rückgabedialogfeld verwendet.

4. Füllen Sie das Feld "Sichere Browsereinstellungen" folgendermaßen aus:

   Standard-URL

   Die Standardseite, zu der navigiert werden soll, wenn für link1_cmd oder link2_cmd keine Befehlszeile angegeben wurde.

   Erlaubnisliste

   Ein reguläres Ausdrucksmuster, das mit URLs übereinstimmt, auf die der Zugriff stets erlaubt werden soll.

   Ausschlussliste

   Ein reguläres Ausdrucksmuster, das mit URLs übereinstimmt, auf die der Zugriff stets verweigert werden soll.

5. (Optional) Klicken Sie auf "Exportieren", um Ihre Einstellungen in ein anderes System zu exportieren.
6. Klicken Sie auf "OK", um Ihre Einstellungen zu speichern.
7. Starten Sie den Rechner neu.

Konfigurieren des Credential Providers

Sie können mit einem Konfigurationstool ein System konfigurieren, auf dem Sie Credential Provider installiert haben.

So konfigurieren Sie Credential Provider:

1. Wechseln Sie im Windows Explorer in das Verzeichnis, in dem der Credential Provider installiert wurde. Beispiel:

   C:\Programme\CA\Identity Manager\Credential Provider

2. Doppelklicken Sie auf die folgende ausführbare Datei:

   CAIMCredProvConfig.exe

3. Füllen Sie das Feld "Credential Provider-Einstellungen" folgendermaßen aus:

   Link1 URL

   Die vollständige Befehlszeile, die ausgeführt wird, wenn der Benutzer auf den Link "Kennwort vergessen" klickt. Dieser Link sollte ein URL zu einer Webschnittstelle zum Zurücksetzen von Kennwörtern sein.

   Beispiel für einen Befehl:

   http://eastern.local:8080/iam/im/pub/ca/index.jsp?task.tag=ForgottenPassword

   Für diese URL muss die Selbstregistrierung in der Umgebung funktionieren. Stellen Sie außerdem sicher, dass die Self-Service-URL für die CA IdentityMinder-Umgebung auf dem System funktioniert, auf dem Sie Credential Provider installieren.

   Link2 **URL**

   Die vollständige Befehlszeile, die ausgeführt wird, wenn der Benutzer auf den Link "Konto entsperren" klickt. Dieser Link sollte ein URL zu einer Webschnittstelle sein, über die der Benutzer ein Konto entsperren kann.

   Link3 URL

   Die vollständige Befehlszeile, die ausgeführt werden soll, wenn der Benutzer auf den Link für ein neues Konto klickt. Dieser Link sollte eine URL zu einer Webschnittstelle sein, über die der Benutzer ein Konto erstellen kann.

   Domäne

   Name der Bereitstellungsdomäne.

   Section 508 Compliance (Use Return in menu) - Konformität mit Abschnitt 508 (Rückgabefunktion im Menü verwenden)

   Aktiviert die Rückgabefunktion in einem Menü. Wenn diese Option nicht ausgewählt ist, wird das Rückgabedialogfeld verwendet.

4. Füllen Sie das Feld "Sichere Browsereinstellungen" folgendermaßen aus:

   Erlaubnisliste

   Ein reguläres Ausdrucksmuster, das mit URLs übereinstimmt, auf die der Zugriff stets erlaubt werden soll.

   Ausschlussliste

   Ein reguläres Ausdrucksmuster, das mit URLs übereinstimmt, auf die der Zugriff stets verweigert werden soll.

5. (Optional) Klicken Sie auf "Exportieren", um Ihre Einstellungen in ein anderes System zu exportieren.

6. Klicken Sie auf "OK", um Ihre Einstellungen zu speichern.

7. Starten Sie den Rechner neu.

Einstellungen in der Registrierung

Obwohl Konfigurationstools für die Einrichtung von GINA oder Credential Provider vorhanden sind, können Sie auch die Windows-Registrierung bearbeiten und so dieselben Werte bereitstellen.

Registrierungseinstellungen für GINA

Wenn Sie das Konfigurationstool für GINA nicht verwenden möchten, können Sie die Windows-Registrierung in folgendem Schlüssel bearbeiten:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\GINAUNLOCK]
```

gina

Dieser Schlüssel enthält den Wert der aktuellen verketteten GINA. Im Allgemeinen ist dies MSGINA.DLL, die Microsoft Windows-Standard-GINA, es sei denn, es hat eine Integration in ein Produkt wie Novell stattgefunden.

link1_cmd

Dies ist die vollständige Befehlszeile, die im Anmeldedialogfeld für Link Nr. 1 ausgeführt werden soll.

link2_cmd

Dies ist die vollständige Befehlszeile, die im Anmeldedialogfeld für den optionalen Link Nr. 2 ausgeführt werden soll. Sie können beispielsweise einen Link hinzufügen, der zu einer Website zum Entsperren von Konten führt.

Wenn link2_cmd freigelassen wurde, wird lediglich link1_cmd im Anmeldedialogfeld angezeigt.

link3_cmd

Die vollständige Befehlszeile, die ausgeführt werden soll, wenn der Benutzer auf den Link für ein neues Konto klickt. Dieser Link sollte eine URL zu einer Webschnittstelle laden, über die der Benutzer ein Konto erstellen kann.

comp508

Aktiviert die Rückgabefunktion in einem Menü. Wenn diese Option nicht ausgewählt ist, wird das Rückgabedialogfeld verwendet.

usecustomtitle

Dies aktiviert den benutzerdefinierten Titel für GINA.

customtitle

Dies ist ein Titel zur Anzeige in GINA.

Domäne

Name der Bereitstellungsdomäne.

langdir

Der Speicherort der lokalisierten Sprach-DLLs.

configdir

Der vollständige Verzeichnispfad zum Installationsverzeichnis von GINA.

rejectinvalidcerts

Steuert, ob GINA nur gültige SSL-Zertifikate akzeptiert. Bei Einstellung auf "no" werden abgelaufene oder ungültige SSL-Zertifikate zugelassen.

Die unterstützten Werte für diesen Schlüssel sind *yes* und *no*.

Registrierungseinstellungen für Credential Provider

Wenn Sie das Konfigurationstool für Credential Provider nicht verwenden möchten, können Sie die Windows-Registrierung in folgendem Schlüssel bearbeiten:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\CA\CAIMCredentialProvider]
```

link1_cmd

Dies ist die vollständige Befehlszeile, die im Anmeldedialogfeld für Link Nr. 1 ausgeführt werden soll. Bei diesem Link sollte es sich um die URL handeln, zu der navigiert werden soll, wenn ein Benutzer auf den ersten Link klickt.

link2_cmd

Dies ist die vollständige Befehlszeile, die im Anmeldedialogfeld für den optionalen Link Nr. 2 ausgeführt werden soll. Bei diesem Link sollte es sich um die URL handeln, zu der navigiert werden soll, wenn ein Benutzer auf den zweiten Link klickt. Sie können beispielsweise einen Link hinzufügen, der zu einer Website zum Entsperren von Konten führt.

Wenn link2_cmd freigelassen wurde, wird lediglich link1_cmd im Anmeldedialogfeld angezeigt.

link3_cmd

Die vollständige Befehlszeile, die ausgeführt werden soll, wenn der Benutzer auf den Link für ein neues Konto klickt. Dieser Link sollte eine URL zu einer Webschnittstelle laden, über die der Benutzer ein Konto erstellen kann.

usecustomtitle

Dies aktiviert den benutzerdefinierten Titel für den Credential Provider.

customtitle

Dies ist ein Titel zur Anzeige im Credential Provider.

comp508

Aktiviert die Rückgabefunktion in einem Menü. Wenn diese Option nicht ausgewählt ist, wird das Rückgabedialogfeld verwendet.

Domäne

Name der Bereitstellungsdomäne.

langdir

Der Speicherort der lokalisierten Sprach-DLLs.

disablepwdcp

Die Option "Credential Provider für Microsoft-Kennwörter deaktivieren". 1 ist deaktiviert. 0 ist aktiviert.

CredentialProviderInstallPath

Der vollständige Verzeichnispfad zum Installationsverzeichnis von Credential Provider.

configdir

Der vollständige Verzeichnispfad zum Installationsverzeichnis von Credential Provider.

rejectinvalidcerts

Steuert, ob der Credential Provider nur gültige SSL-Zertifikate akzeptiert. Bei Einstellung auf "no" werden abgelaufene oder ungültige SSL-Zertifikate zugelassen.

Die unterstützten Werte für diesen Schlüssel sind *yes* und *no*.

Registrierungseinstellungen für den Cube-Browser

Die sichere Cube-Browserkomponente weist zahlreiche Registrierungswerte auf, die ihr Verhalten steuern. Die Cube-Werte befinden sich im folgenden Registrierungsschlüssel:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Cube]
```

404

Der Pfad zu einem Standard-HTML-Dokument, das angezeigt werden soll, wenn der Rechner beim Systemstart keinen Kontakt zum entfernten Bereitstellungsserver herstellen kann.

default

Die Standardseite, zu der navigiert werden soll, wenn sich im Befehl Link1 oder Link2 keine URL befindet.

allow

Ausdrückliche Erlaubnis von Zugriffssteuerungslisten. Ein reguläres Ausdrucksmuster, das mit URLs übereinstimmt, auf die der Zugriff immer erlaubt ist. Weitere Informationen finden Sie in den Cube-Zugriffssteuerungslisten (siehe Seite 126).

deny

Ausdrückliche Ablehnung von Zugriffssteuerungslisten. Ein reguläres Ausdrucksmuster, das mit URLs übereinstimmt, auf die der Zugriff stets verweigert werden soll. Weitere Informationen finden Sie in den Cube-Zugriffssteuerungslisten (siehe Seite 126).

langdir

Der Speicherort der lokalisierten Sprach-DLLs.

Cube-Zugriffssteuerungslisten

Cube-Zugriffssteuerungslisten sind reguläre Ausdrucksmuster, die das Navigieren zu einer ausgewählten URL ausdrücklich erlauben oder verweigern. Zugriffssteuerungslisten werten in der folgenden Reihenfolge aus:

1. Erlauben (die Erlaubnis wird automatisch als erstes gewährt)
2. Ablehnen (abgelehnte URLs werden als nächstes überprüft)

Beispiele für GINA-Zugriffssteuerungslisten

"erlauben"="(.pdf)"

Hiermit wird die Anzeige aller PDF-Dokumente erlaubt.

"ablehnen"="(.doc|.xls)"

Hiermit wird der Zugriff auf Microsoft Word- und Excel-Dokumente verweigert.

Anpassen der "Powered By"-Meldung

Sie stellen möglicherweise eine "Powered By"-Meldung im Rückgabedialogfeld oder der Rückgabe-Menüoption von GINA oder dem Credential Provider fest. Sie können diese Meldung bearbeiten oder entfernen.

So passen Sie die "Powered By"-Meldung an

1. Laden Sie ResEdit, einen Freeware-Ressourceneditor, von http://www.resedit.net herunter.
2. Starten Sie ResEdit.
3. Bearbeiten Sie die Datei 1033.dll im Sprachordner.
4. Doppelklicken Sie auf die Zeichenfolgentabelle.
5. Entfernen oder ändern Sie Ressourcen-ID 135, die englische Ressourcenversion für diese Meldung.

Zurücksetzen eines Kennwortes für eine Windows-Anmeldung

Nachdem GINA oder Credential Provider auf einem Windows-System installiert wurden, wird im standardmäßigen Microsoft Windows-Anmeldedialogfeld der Link "Kennwort vergessen" angezeigt. Über diesen Link können Sie Ihr Kennwort zurücksetzen oder Kennworthinweise anzeigen, die Ihnen dabei helfen, sich an das Kennwort zu erinnern.

So setzen Sie ein Kennwort für eine Windows-Anmeldung zurück:

1. Klicken Sie im Dialogfeld "Windows-Sicherheit" auf "Anmelden". Das Windows-Anmeldedialogfeld wird angezeigt.
2. Geben Sie einen gültigen Benutzernamen ein.
3. Klicken Sie auf "Kennwort vergessen".

   Die Seite CA IdentityMinder "Kennworthinweis" wird angezeigt.

   Falls Sie sich an Ihr Kennwort erinnern können, kehren Sie zum Anmeldedialogfeld zurück, um fortzufahren. Andernfalls führen Sie Schritt 4 durch, um sich gegenüber CA IdentityMinder-Self-Service zu authentifizieren.
4. Geben Sie die Antworten auf die Authentifizierungsfragen ein.

   Hinweis: Wenn Sie nicht auf alle Fragen die Antworten kennen, können Sie auf "Anfrage" klicken, damit Ihr Kennwort von einem Administrator zurückgesetzt werden kann.
5. Wenn Sie die Fragen beantworten können, klicken Sie auf "Anmelden".

   Sie werden angemeldet, und Self-Service wird geöffnet.
6. Ändern Sie Ihr Kennwort.
7. Kehren Sie zum Anmeldedialogfeld zurück, und melden Sie sich mit Ihrem neuen Kennwort an.

Automatische GINA-Installation

GINA unterstützt einen automatischen Installationsmodus. Es werden sechs Eigenschaften unterstützt:

LINK1

Verweist auf SOFTWARE\ComputerAssociates\GINAUNLOCK\link1_cmd in der Registrierung.

LINK2

Verweist auf SOFTWARE\ComputerAssociates\GINAUNLOCK\link2_cmd in der Registrierung.

LINK3

Verweist auf SOFTWARE\ComputerAssociates\GINAUNLOCK\link3_cmd in der Registrierung.

GNADOMAIN

Verweist auf SOFTWARE\ComputerAssociates\GINAUNLOCK\domain in der Registrierung.

COMP508

Verweist auf SOFTWARE\ComputerAssociates\GINAUNLOCK\comp508 in der Registrierung.

USECUSTOMTITLE

Verweist auf SOFTWARE\ComputerAssociates\Cube\usecustomtitle in der Registrierung.

CUSTOMTITLE

Verweist auf SOFTWARE\ComputerAssociates\Cube\customtitle in der Registrierung.

REJECTINVALIDCERTS

Verweist auf SOFTWARE\ComputerAssociates\Cube\rejectinvalidcerts in der Registrierung.

UNREACHABLE

Verweist auf den Speicherort der nicht erreichbaren Seite.

Die Syntax, um den Wert dieser Eigenschaften festzulegen, ist wie folgt:

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Programme\CA\Identity
Manager\Provisioning GINA\" LINK1=\"[INSTALLDIR]cube <url>\"
LINK2=\"[INSTALLDIR]cube <url>\" LINK3=\"[INSTALLDIR]cube <url>\"
COMP508=\"yes\" REJECTINVALIDCERTS=\"yes\" USECUSTOMTITLE=\"yes\"
CUSTOMTITLE=\"angepasster gina-titel\""
```

oder

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Programme\CA\Identity
Manager\Provisioning GINA\" LINK1=\"[INSTALLDIR]cube <url>\"
LINK2=\"[INSTALLDIR]cube <url>\" LINK3=\"[INSTALLDIR]cube <url>\"
COMP508=\"yes\" USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"angepasster
gina-titel\" SELECTDEFAULTCREDENTIAL=\"yes\" UNREACHABLE=\"<url>\""
```

oder

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Program
Files\CA\Identity Manager\Provisioning GINA\"
LINK1=\"[INSTALLDIR]cube <url>\" LINK2=\"[INSTALLDIR]cube <url>\"
LINK3=\"[INSTALLDIR]cube <url>\" COMP508=\"yes\"
USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"custom gina title\"
SELECTDEFAULTCREDENTIAL=\"yes\"
UNREACHABLE=\"file:///[INSTALLDIR]<file name>\" GNAALLOW=\"\"
GNADENY=\"\""
```

[INSTALLDIR]

Verweist auf den Wert der INSTALLDIR-Eigenschaft.

<url>

Gibt die URL für eine Aufgabe des Typs "Konten entsperren" oder "Kennwort vergessen" an.

<Dateiname>

Definiert den Namen der nicht erreichbaren Datei.

GNAALLOW

Der URL-Aufruf von Cube ist zulässig.

GNADENY

Der URL-Aufruf von Cube ist eingeschränkt.

Automatische Credential Provider-Installation

Der Credential Provider unterstützt einen automatischen Installationsmodus. Es werden sechs Eigenschaften unterstützt.

LINK1

Verweist auf SOFTWARE\CA\CAIMCredentialProvider\link1_cmd in der Registrierung.

LINK2

Verweist auf SOFTWARE\CA\CAIMCredentialProvider\link2_cmd in der Registrierung.

LINK3

Verweist auf SOFTWARE\CA\CAIMCredentialProvider\link3_cmd in der Registrierung.

DOMAIN

Verweist auf SOFTWARE\CA\CAIMCredentialProvider\domain in der Registrierung.

COMP508

Verweist auf SOFTWARE\CA\CAIMCredentialProvider\comp508 in der Registrierung.

USECUSTOMTITLE

Verweist auf SOFTWARE\CA\Cube\usecustomtitle in der Registrierung.

CUSTOMTITLE

verweist auf SOFTWARE\CA\Cube\customtitle in der Registrierung.

REJECTINVALIDCERTS

verweist auf SOFTWARE\ComputerAssociates\Cube\rejectinvalidcerts in der Registrierung.

UNREACHABLE

Verweist auf den Speicherort der nicht erreichbaren Seite.

Die Syntax, um den Wert dieser Eigenschaften festzulegen, ist wie folgt:

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Programme\CA\Identity
Manager\Credential Provider\" LINK1=\"<url>\" LINK2=\"<url>\"LINK3=\"<url>\"
COMP508=\"yes\" REJECTINVALIDCERTS=\"yes\" USECUSTOMTITLE=\"yes\"
CUSTOMTITLE=\"angepasster cp-titel\""
```

oder

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Programme\CA\Identity
Manager\Credential Provider\" LINK1=\"<url>\" LINK2=\"<url>\" LINK3=\"<url>\"
COMP508=\"yes\" USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"angepasster cp-titel\"
SELECTDEFAULTCREDENTIAL=\"yes\" UNREACHABLE=\"<url>\""
```

oder

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Programme\CA\Identity
Manager\Credential Provider\"
LINK1=\"<url>\" LINK2=\" <url>\" LINK3=\"<url>\" COMP508=\"yes\"
USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"custom cp title\"
SELECTDEFAULTCREDENTIAL=\"yes\" UNREACHABLE=\"file:///[INSTALLDIR]<file
name>\"CUBE_ALLOW=\"\"CUBE_DENY=\"\""
```

[INSTALLDIR]

Verweist auf den Wert der INSTALLDIR-Eigenschaft.

<url>

Gibt die URL für eine Aufgabe des Typs "Konten entsperren" oder "Kennwort vergessen" an.

<Dateiname>

Definiert den Namen der nicht erreichbaren Datei.

CUBE_ALLOW

Der URL-Aufruf von Cube ist zulässig.

CUBE_DENY

Der URL-Aufruf von Cube ist eingeschränkt.

Kapitel 6: Synchronisieren von Kennwörtern auf Endpunkten

Sie können einen Agenten für die Kennwortsynchronisierung auf bestimmten Endpunkten installieren, die von CA IdentityMinder unterstützt werden. Der Agent fängt Kennwortänderungsanfragen auf dem Endpunkt ab und sendet die Änderungen an den Bereitstellungsserver.

Dieses Kapitel enthält folgende Themen:

Kennwortsynchronisierung unter Windows (siehe Seite 133)
Kennwortsynchronisierung unter UNIX und Linux (siehe Seite 144)
Kennwortsynchronisierung auf OS400 (siehe Seite 159)

Kennwortsynchronisierung unter Windows

CA IdentityMinder kann die Kennwortänderung für ein systemeigenes Windows-Konto abfangen und das neue Kennwort an einen Benutzer und alle zu diesem Benutzer gehörenden Konten übertragen.

Wenn der Agent für die Kennwortsynchronisierung den Versuch einer Kennwortänderung entdeckt, fängt der Agent die Anfrage ab und sendet sie an den Bereitstellungsserver. Der Bereitstellungsserver überträgt dann das neue Kennwort an den Benutzer und andere diesem Benutzer zugeordnete Konten.

Für die Kennwortsynchronisierung bestehen die folgenden Anforderungen:

- Der Agent für die Kennwortsynchronisierung muss auf dem System installiert sein, auf dem die Kennwortänderungen abgefangen werden.
- Das System muss als ein erfasster Endpunkt verwaltet werden.
- Das Kontrollkästchen "Agent für die Kennwortsynchronisierung ist installiert" muss auf der Registerkarte "Endpunkteinstellungen" für den erfassten Endpunkt aktiviert sein.
- Die Konten auf den verwalteten Systemen müssen für Benutzer von CA IdentityMinder durchsucht und korreliert werden.
- Die Umgebung muss so eingerichtet sein, dass Kennwortänderungen aus Endpunktkonten akzeptiert werden. Diese Funktion wird von einem Administrator mit Zugriff auf die Management-Konsole aktiviert.

Wichtig! Achten Sie beim Formulieren der Kennwortregeln darauf, dass ein Kennwort auf allen Systemen gültig ist. Wenn z. B. Windows-Kennwörter 12 Zeichen lang sein müssen, dann wird die Änderung während der Synchronisierung von allen Systemen abgelehnt, die nur Kennwörter bis zu einer Länge von 10 Zeichen akzeptieren.

Der CA IdentityMinder-Server kennt die Kennworteinschränkungen auf dem Endpunkt nicht. Wenn Sie mit Endpunktkonten arbeiten, sollte die Kennwortrichtlinie strenger als die Kennwortrichtlinie auf den Endpunkten sein.

Installieren des Agenten für die Kennwortsynchronisierung

Sie können den Agenten für die Kennwortsynchronisierung auf einem beliebigen verwalteten Windows-Computer installieren, auf dem sich globale Benutzer anmelden. Auf diesen Computern läuft der Agent im Hintergrund.

Ausführen des Installationsprogramms

Beachten Sie die folgenden Anforderungen:

- Der Bereitstellungsserver muss das System verwalten, auf dem Sie den Agenten installieren.
- Erstellen Sie einen Benutzer, der als Administrator für Kennwortänderungen fungieren soll: Der vorgeschlagene Name ist "etapwsad". Dieser Benutzer muss das Profil "PasswordAdministrator" haben.
- Zwei Agenten für die Windows-Kennwortsynchronisierung sind in den Installationsdatenträgern vorhanden: einer für 32-Bit-Windows und einer für 64-Bit. Der 32-Bit-Kennwortsynchronisierungs-Agent wird nicht auf 64-Bit-Windows unterstützt. FIPS wird nur vom 32-Bit-Kennwortsynchronisierungs-Agenten unterstützt.

Gehen Sie wie folgt vor:

1. Suchen Sie nach dem CA IdentityMinder-Installationsdatenträger.
2. Navigieren Sie zu "\Agent\PasswordSync" oder "\Agent\PasswordSync-x64".
3. Führen Sie setup.exe aus.
4. Gehen Sie im Konfigurationsassistenten folgendermaßen vor:
   a. Geben Sie im Feld "Hostname" den Namen des Systems ein, das als Bereitstellungsserver dient.

b. Ändern Sie ggf. den Port, wenn die Bereitstellungsserver-Installation einen nicht standardmäßigen Port verwendet.

   Als LDAP-Port, der für die Herstellung einer Verbindung mit dem Bereitstellungsserver verwendet wird, wird 20390 empfohlen.

c. Klicken Sie auf die Schaltfläche "Find domain" (Domäne suchen), um die Domäne des Bereitstellungsservers abzurufen.

d. Wenn die Bereitstellungsserver-Installation für Failover konfiguriert ist, folgen Sie den Bildschirmanweisungen, um eine durch Kommas getrennte Liste von Servern hinzuzufügen.

e. Klicken Sie auf "Weiter".

f. Geben Sie im Feld "Administrator" den Namen "etapwsad" als standardmäßigen globalen Benutzernamen für den Agenten für die Kennwortsynchronisierung ein. Dieser Benutzer muss das Profil "PasswordAdministrator" haben. Es ist nicht standardmäßig vorhanden.

g. Geben Sie im Feld "Password Administrator" (Administratorkennwort) das Kennwort des Administrators ein.

h. Klicken Sie auf "Weiter".

i. Wählen Sie in der Drop-down-Liste "Endpunkttyp" den Endpunkttyp des Hosts aus, auf dem Sie den Agenten installieren.

j. Wählen Sie in der Drop-down-Liste "Endpunktname" den Endpunktnamen aus, der bei der Erstellung des Endpunkts in der Benutzerkonsole verwendet wurde.

k. Klicken Sie auf "Konfigurieren".

5. Klicken Sie auf "Fertig stellen", um die Installation abzuschließen, und führen Sie einen Neustart durch.

Aktualisieren des Endpunkts in der Benutzerkonsole

Aktualisieren Sie den Endpunkt in der Benutzerkonsole, um anzuzeigen, dass der Agent installiert wird.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole an.
2. Klicken Sie auf "Endpunkte", "Manage Endpoints" (Endpunkte verwalten), "Endpunkt ändern".
3. Suchen Sie nach dem Endpunkt, auf dem der Agent installiert ist.
4. Klicken Sie auf die Registerkarte "Endpunkteinstellungen".
5. Aktivieren Sie das Kontrollkästchen "Agent für die Kennwortsynchronisierung ist installiert".

Aktivieren einer Umgebung für die Kennwortsynchronisierung

Nachdem Sie den Agenten für die Kennwortsynchronisierung installiert haben, aktivieren Sie die Umgebung für den Eingang von Kennwortänderungen, die auf den Endpunkten vorgenommen wurden. Der Administrator benötigt für diese Aufgabe Zugriff auf die Management-Konsole und CA Directory, um die Umgebung so einzurichten, dass diese Änderungen akzeptiert werden.

Gehen Sie wie folgt vor:

1. Für neue Benutzer verwenden Sie die Management-Konsole folgendermaßen:
   a. Wählen Sie die Umgebung aus.
   b. Klicken Sie auf "Advanced Settings" (Erweiterte Einstellungen), "Provisioning" (Bereitstellung).
   c. Aktivieren Sie das Kontrollkästchen "Enable Password Changes from Endpoint Accounts" (Kennwortänderungen auf Endpunktkonten aktivieren).
2. Legen Sie das Attribut "eTPropagatePassword" in CA Directory für vorhandene Benutzer auf "1" fest.

Konfiguration alternativer Server für den Agenten für die Kennwortsynchronisierung

Mit Hilfe des Konfigurationsassistenten für den Agenten für die Kennwortsynchronisierung können Sie einen alternativen Server für den Agenten für die Kennwortsynchronisierung konfigurieren.

So fügen Sie einen alternativen Server für den Agenten für die Kennwortsynchronisierung hinzu

1. Führen Sie die Datei PwdSyncConfig.exe aus, die Sie im Ordner "*password_sync_folder*\bin" finden.
2. Geben Sie folgende Konfigurationsdaten ein:

   Host

   Geben Sie den Hostnamen des primären Bereitstellungsservers ein.

   Dadurch wird das Feld für die Server-URL mit dem von Ihnen angegebenen Hostnamen ausgefüllt.

   LDAP-Port

   Geben Sie die Portnummer an, die der Computer für die Verbindung mit dem Bereitstellungsserver verwendet.

   CA IdentityMinder füllt das Feld für die Server-URL mit dem von Ihnen angegebenen Hostnamen und Port aus.
3. Klicken Sie auf die Schaltfläche "Find domain" (Domäne suchen), um die Domänenliste aufzurufen.

4. Wählen Sie im Dropdown-Feld "Domäne" den Namen der Domäne aus, und klicken Sie auf "Weiter".
5. Geben Sie den Hostnamen und den Port der alternativen Server in folgendem Format im Feld für die Server-URLs ein:

   ldaps://*primaryhost*:20390,ldaps://*alternatehost1*:20390
6. Klicken Sie auf "Weiter".
7. Füllen Sie die verbleibenden Felder im Konfigurationsassistenten aus.

Funktionsweise des Agenten für die Kennwortsynchronisierung

Der Propagierungsprozess beginnt, wenn globale Benutzer unter Verwendung einer beliebigen Methode auf einem Windows-System ihre Kennwörter ändern. Nach der Eingabe des Kennworts, passiert das Folgende:

1. Das Windows-Betriebssystem führt Prüfungen durch, um sicherzustellen, dass das Kennwort die Kennwortrichtlinie erfüllt. Wenn Windows das Kennwort nicht akzeptiert, wird der Änderungsantrag abgelehnt, eine Fehlermeldung wird angezeigt, und es werden keine weiteren Maßnahmen, einschließlich Synchronisierung, unternommen.
2. Das Windows-System übergibt den Kennwortänderungsantrag an den Agenten für die Kennwortsynchronisierung CA IdentityMinder, der bei konfigurierter Kennwortqualitätsprüfung das Kennwort an den Bereitstellungsserver sendet, um die Kennwortqualitätsprüfung durchzuführen. Wenn das Kennwort die Qualitätsregeln von CA IdentityMinder nicht erfüllt, wird der Änderungsantrag abgelehnt, und eine Fehlermeldung wird angezeigt. Das Windows-Kennwort wird nicht geändert und es wird keine Synchronisierung durchgeführt.
3. Ein Kennwort, das die Qualitätsregeln von Windows und CA IdentityMinder erfüllt, wird vom Agenten für die Kennwortsynchronisierung an den Bereitstellungsserver zur Propagierung gesendet.
4. CA IdentityMinder aktualisiert das Kennwort des globalen Benutzers und verbreitet das neue Kennwort an einige oder alle Konten, die dem globalen Benutzer zugeordnet sind.

Hinweis: Die Kennwortrichtlinien für Windows und CA IdentityMinder müssen identisch oder konsistent sein, weil die angezeigten Fehlermeldungen auf der Kennwortrichtlinie von Windows basieren, selbst dann, wenn CA IdentityMinder den Antrag ablehnt.

Der Konfigurationsparameter "password_update_timeout" (eta_pwdsync.conf) legt fest, wie lange (in Sekunden) der PSA auf die Bestätigung der Kennwortänderung vom CA IdentityMinder-Server wartet. Wenn während dieser Zeit keine Bestätigung empfangen wird, fährt der PSA fort, als wäre die Propagierung erfolgreich verlaufen. Eine Warnung wird protokolliert (eta_pwdsync.log), dass die Propagierung der Kennwortänderung nicht verifiziert werden konnte. Der Mindestwert für den Parameter ist Null (0), d. h. der PSA wartet nicht auf eine Bestätigung. Weitere Informationen hierzu finden Sie in der Hilfe zu eta_pwdsync.conf--Konfigurieren des Agenten für die Kennwortsynchronisierung im Bereitstellungs-Manager.

Kennwortqualitätsprüfung auf Kontoebene

Die Kennwortqualitätsprüfung wird durchgeführt, wenn Konten auf verwalteten Endgeräten erstellt oder geändert oder globale Benutzerkennwörter festgelegt werden. Die Kennwortqualitätsprüfung auf Konten beschränkt sich auf Prüfungen, die auf den Zeichen des Kennworts basieren. Prüfungen auf globale Benutzer, die auf dem Verlauf der letzten Änderungen (Häufigkeit der Kennwortaktualisierungen und Häufigkeit der Wiederverwendung des Kennworts) basieren, werden nicht auf den Konten durchgeführt, weil CA IdentityMinder nicht alle Kennwortänderungen für Kontokennwörter abfängt. Aus diesem Grund gibt es keinen genauen Verlauf der Kennwortänderungen, der als Grundlage für diese Prüfungen verwendet werden könnte.

Die Überprüfung der Kontokennwörter wird durch die folgenden Konfigurationsparameter für Domänen gesteuert:

- Endpunkttyp/Kontokennwörter prüfen
- Endpunkttyp/Leere Kontokennwörter prüfen

Der Wert für jeden Parameter legt für jedes verwaltete Endgerät die Ebene der Prüfungen fest, die durchgeführt werden sollen. Das Endgerät kann auf die folgenden Arten festgelegt werden:

```
ALLE
-ALLE
<NamespaceName>
-<NamespaceName>
<NamespaceName>:<DirectoryName>
-<NamespaceName>:<DirectoryName>
```

Formulare mit einem Minuszeichen (-) deaktivieren den Parameter. Formulare ohne ein Minuszeichen aktivieren den Parameter. Die [-]<NamespaceName>-Formulare steuern alle Endpunkte des angegebenen Endpunkttyps, während die [-]<NamespaceName>:<DirectoryName>-Formulare individuelle Endpunkte steuern. Die [-]ALLE-Formulare steuern alle Endpunkte aller Endpunkttypen. Der Standardwert für beide Parameter ist -ALLE.

Jeder dieser Parameter kann mehrfach angegeben werden. Wenn unterschiedliche Werte dasselbe Endgerät angeben, wird der letzte Wert verwendet. Sie können allgemeine Regeln zuerst und spezielle Regeln später angeben, um die allgemeine Regel außer Kraft zu setzen.

Der Parameter "Kontokennwörter prüfen" stellt dieselben Prüfungen bereit wie die Kennwortqualitätsprüfung für globale Benutzer. Wenn dieser Parameter für einen Endpunkt aktiviert ist, werden alle Kennwörter in einer gewünschten Änderung für ein bestehendes Konto von CA IdentityMinder überprüft, einschließlich eines leeren Kennworts. Wird beim Erstellen eines Kontos kein Kennwort angegeben, wird keine Kennwortqualitätsprüfung durchgeführt.

"Leere Kontokennwörter prüfen" führt eine weitere Überprüfung nach leeren Kennwörtern durch, wenn Konten erstellt werden. Wenn das Kennwortprofil aktiviert und als Mindestanforderung ein Kennwort mit Länge von einem Zeichen erforderlich ist, schlägt die Erstellung des Kontos fehl. Dieser Parameter unterscheidet sich von "Kontokennwörter prüfen", weil für einige Endpunkttypen das Erstellen von Konten ohne Kennwörtern zulässig ist.

Hinweis: Die Kennwortqualitätsprüfung für Konten wird für synchronisierte Kontokennwörter übersprungen, wenn das bereitgestellte Kennwort mit dem aktuellen Kennwort des globalen Benutzers übereinstimmt.

Durchsetzung der Kennwortqualität

Die Option für die Kennwortsynchronisierung fängt Kennwortänderungsanträge auf systemeigenen Systemen (z. B, Windows NT/ADS) ab und sendet diese an den CA IdentityMinder-Server. Der Server synchronisiert das Kennwort des globalen Benutzers und die Kontokennwörter, die mit dem globalen Benutzer verbunden sind. Die Regeln für die Kennwortqualität von CA IdentityMinder für ein Kennwortprofil und die des systemeigenen Systems (Windows NT/ADS) können verwendet werden, um die Kennwortqualitätsprüfung durchzusetzen.

Konfigurieren der Kennwortsynchronisierung

Der Agent für die Kennwortsynchronisierung wird erstmals während der Installation konfiguriert und kann jederzeit mithilfe des Konfigurationsassistenten für die Kennwortsynchronisierung neu konfiguriert werden. Weitere Konfigurationen sind möglich. Sie können zum Beispiel die Einstellungen für die Überprüfung der Kennwortqualität oder die Änderung von Zeitlimits über die Datei "eta_pwdsync.conf" ändern.

Diese Datei befindet sich im Ordner "password_sync_folder\data\". Alle Schlüssel in dieser Konfigurationsdatei werden während der Installation des Agenten für die Kennwortsynchronisierung festgelegt. Ändern Sie diese Schlüssel deswegen nur, wenn erforderlich. Weitere Informationen finden Sie im Text dieser Datei.

Wichtig! Erstellen Sie vorsichtshalber eine Sicherung der Konfigurationsdatei, bevor Sie sie bearbeiten.

[Server]-Abschnitt

Schlüssel	Beschreibung	Standard
Host	Gibt den Domänenserver an, der die Kennwortpropagierung verwaltet.	Keine
port	Gibt den LDAP-Listener-Port des Bereitstellungsservers an.	20411
use_tls	Gibt an, ob TLS/SSL verwendet wird, um die Kommunikation zwischen dem Agenten für die Kennwortsynchronisierung und dem Bereitstellungsserver zu sichern.	Ja
admin_suffix	Gibt das Domänensuffix des Admin-Benutzers an, den der Agent für die Kennwortsynchronisierung verwendet, um sich bei CA IdentityMinder anzumelden.	Keine
admin	Gibt den Kontonamen des Admin-Benutzers an, den der Agent für die Kennwortsynchronisierung verwendet, um sich bei CA IdentityMinder anzumelden.	Keine
password	Gibt das Kennwort für den im Admin-Schlüssel angegebenen Kontonamen an.	Keine

[eTaDomain]-Abschnitt

Schlüssel	Beschreibung	Standard
Domäne	Gibt die Bereitstellungsdomäne an, in der Sie den Agenten für die Kennwortsynchronisierung installiert haben.	Keine
etrust_suffix	Gibt das Suffix für das gesamte CA IdentityMinder-Produkt an.	Keine
domain_suffix	Gibt das Domänensuffix für die Bereitstellungsdomäne an.	Keine
endpoint type	Gibt den Typ des Endpunkts an, auf dem Sie den Agenten für die Kennwortsynchronisierung installiert haben.	Keine
endpoint	Gibt den Endpunkt an, für den der Agent für die Kennwortsynchronisierung Kennwörter abfängt.	Keine
endpoint_dn	Gibt den Distinguished Name des Endpunkts an.	Keine
container_dn	Gibt den Distinguished Name des Containers an, der die Konten enthält, deren Kennwörter geändert werden.	Keine
acct_attribute_name	Gibt den Attributnamen des Kontos an, zum Beispiel eTN16AccountName für Windows NT.	Abhängig vom Endpunkttyp
acct_object_class	Gibt die Objektklasse des Kontos an.	Abhängig vom Endpunkttyp

[PasswordProfile]-Abschnitt

Schlüssel	Beschreibung	Standard
profile_enabled	Gibt an, ob die Funktion zum Prüfen des Kennwortprofils aktiviert ist.	Nein
profile_dn	Gibt an, ob der Assistent für die Kennwortkonfiguration einen DN für das Kennwortprofil generiert.	eTPasswordProfileName=Password Profile,eTPasswordProfileContainerName=Password Profile,eTNamespaceName=CommonObjects,dc=cai,dc=eta

[Timeout]-Abschnitt

Schlüssel	Beschreibung	Standard
search_acct_dn	Gibt den Wert für das Zeitlimit bei der Suche nach dem Konto-DN an.	120 Sekunden
pwd_update	Gibt den Wert für das Zeitlimit bei der Kennwortpropagierung an.	400 Sekunden
pwd_quality_check	Gibt den Wert für das Zeitlimit (in Sekunden) bei der Überprüfung der Kennwortqualität an.	1

[Logs]-Abschnitt

Schlüssel	Beschreibung	Standard
log_file	Gibt die Protokolldatei an, die protokollierte Meldungen vom Agenten für die Kennwortsynchronisierung enthält.	..\Programme\CA\Identity Manager Password Sync Agent
log_level	Gibt die Protokollierungsstufe an. Folgende Werte sind gültig: 1--Init-Datei 2--Erfolgreiche oder fehlgeschlagene Kennwortaktualisierung 3--Behebung von Verbindungsfehlern 4--Verfolgung	0, keine Protokollierung

Failover

Wenn der Bereitstellungsserver außer Betrieb oder stark ausgelastet ist, kann der Agent für die Kennwortsynchronisierung auf einem anderen Server ausgeführt werden. Für den Failover ist erforderlich, dass mehrere Bereitstellungsserver für die gleiche Domäne eingesetzt werden und der Agent diese Server verwendet.

Die Konfigurationsanweisungen finden Sie im Abschnitt über das Konfigurieren des Agenten für die Verwendung alternativer Server (siehe Seite 136).

Protokollmeldungen aktivieren

Um festzustellen, warum eine Kennwortänderung abgelehnt wurde, zeigen Sie die Protokollmeldungen an, die vom Agenten für die Kennwortsynchronisierung gesendet wurden. Alle protokollierten Meldungen werden in der Datei eta_pwdsync.log gespeichert. Standardmäßig befindet sich diese Datei im Ordner ..\Programme\CA\CA IdentityMinder Password Sync Agent.

PSA-Protokollierung (in die Datei eta_pwdsync.log) hat die folgenden Meldungen:

- Fehlermeldungen, die immer protokolliert werden.
- Diagnosemeldungen (Prozessablauf, Verfolgung), die auf Grundlage des Parameterwerts von logging_enabled=yes|no in der Datei "eta_pwdsync.conf" aktiviert oder deaktiviert werden können.

Damit Sie Probleme besser diagnostizieren können, überprüfen Sie die Datei eta_pwdsync.log und das Protokoll für den Bereitstellungsserver für denselben Zeitraum.

Der frühere log_level-Konfigurationsparameter ist veraltet, wird jedoch aus Gründen der Rückwärtskompatibilität weiter beibehalten: "log_level=0" entspricht "logging_enabled=no" und "log_level=beliebiger anderer Wert" entspricht "logging_enabled=yes". Wenn die Konfigurationsdatei sowohl alte als auch neue Parameter enthält, überschreibt die explizite Einstellung des Parameters "logging_enabled=yes|no" die indirekte Einstellung, die durch den alten Wert "log_level=Zahl" festgelegt wurde.

Hinweis: Die Liste der verfügbaren Connectors war in der Datei "eta_pwdsync.log" enthalten, aber diese Informationen werden nicht mehr vom Agenten bereitgestellt.

Überprüfen der Installation

Nach Abschluss der Installation des Agenten für die Kennwortsynchronisierung ändern Sie ein Kennwort auf dem Windows-System, um zu verifizieren, dass das Kennwort des globalen Benutzers, das mit dem Konto verbunden ist, ebenfalls geändert wird.

Kennwortsynchronisierung unter UNIX und Linux

CA IdentityMinder kann die Kennwortänderung eines Kontos auf einem UNIX- oder Linux-System abfangen und an alle anderen Konten übertragen, die dem globalen Benutzer zugeordnet sind. Die Komponente, die für die Authentifizierung von Kennwörtern bei externen Sicherheitssystemen verwendet wird, wird als Pluggable Authentication Module (PAM) bezeichnet. Mit PAM authentifiziert CA IdentityMinder Kennwörter bei externen Sicherheitssystemen, sodass globale Benutzer ihre vorhandenen Systemkennwörter verwenden können, um sich bei CA IdentityMinder anzumelden.

UNIX-Kennwortsynchronisierung

Ein Modul für die Kennwortsynchronisierung wird bereitgestellt, das Kennwortänderungsereignisse über das UNIX PAM-Framework erkennt. Das UNIX-Kennwortsynchronisierungs-Modul benachrichtigt den Bereitstellungsserver, wenn ein Kennwort geändert wurde. Der Bereitstellungsserver findet den zugeordneten globalen Benutzer und überträgt die Änderungen automatisch an andere zugehörige Konten.

Die UNIX-Betriebssysteme, die das PAM-Framework unterstützen, umfassen:

- AIX v5.3 auf einer Power-Plattform mit aktiviertem PAM
- HP-UX v11.00 auf einer PA-RISC-Plattform und Itanium® 2-Plattformen
- Solaris v2.6 und höher auf Sparc- und Intel-Plattformen
- 32-Bit-Linux mit glibc v2.2 und höher auf einer s390- oder Intel i386-Plattform

  Hinweis: Bei Linux-Plattformen muss sich die test_sync-Binärdatei im PFAD für alle Benutzer befinden, aber nur der Root-Benutzer, der Eigentümer, sollte die Berechtigung zum Ausführen haben.

  Um diese Bibliothek dem Pfad für alle Benutzer hinzuzufügen, nehmen Sie diesen Befehl in die globale Datei "/etc/bashrc" auf:

  ```
  export PATH=$PATH:/etc/pam_CA_eta
  ```

Funktionsweise von UNIX PAM

Der folgende Prozess stellt eine Beschreibung der UNIX PAM-Funktionen dar:

1. Das Kennwort eines UNIX-Benutzers soll aus einem der folgenden Gründe geändert werden:
   - Entscheidung des Benutzers.
   - Der Benutzer muss das Kennwort aufgrund der Systemeinstellungen oder eines manuellen Eingreifens ändern.
   - Das Kennwort des Benutzers wird von einem Administrator geändert.
2. Das neue Kennwort wird an den Kennwort-Service des PAM-Frameworks gesendet.
3. Der Kennwort-Service des PAM-Frameworks startet die Aktualisierung der lokalen UNIX-Sicherheitsdateien mithilfe der PAM-Bibliothek.
4. Der Kennwort-Service des PAM-Frameworks startet das UNIX-Kennwortsynchronisierungs-Modul (pam_CA_eta), um den Bereitstellungsserver davon zu benachrichtigen, dass das Kennwort geändert wurde.
5. Der Bereitstellungsserver aktualisiert das Kennwort des zugeordneten globalen Benutzers und alle dem globalen Benutzer zugeordneten Konten.

Anforderungen für die Verwendung der UNIX-Kennwortsynchronisierung

Für die Verwendung der UNIX-Kennwortsynchronisierungs-Funktion bestehen die folgenden Anforderungen:

- Der UNIX-Kennwortsynchronisierungs-Agent muss auf dem UNIX-System installiert sein, auf dem Kennwortänderungen erkannt werden sollen.
- Der UNIX-Remote-Agent und CAM müssen auf dem UNIX-System installiert sein, auf dem sich der UNIX-Kennwortsynchronisierungs-Agent befindet.
- Das System muss als ein erfasster Endpunkt verwaltet werden. Das Kontrollkästchen "Agent für die Kennwortsynchronisierung ist installiert" muss in den Eigenschaften für den erfassten Endpunkt aktiviert sein.
- Die Konten auf den verwalteten Systemen müssen für globale Benutzer durchsucht und korreliert werden.
- Die Umgebung muss so eingerichtet sein, dass Kennwortänderungen aus Endpunktkonten akzeptiert werden. Diese Funktion wird von einem Administrator mit Zugriff auf die Management-Konsole aktiviert.

Installieren der UNIX PAM-Funktion

Gehen Sie folgendermaßen vor, um UNIX PAM zu installieren.

So installieren Sie die UNIX PAM-Funktion

1. Wählen Sie die Paketdatei aus, die Ihrer UNIX-Plattform entspricht:

UNIX-Betriebssystem	Paket-Dateiname
HP-UX v11 PA-RISC	pam_CA_eta-1.1.HPUX.tar.Z
HP-UX Itanium2	pam_CA_eta1.1HPUX-IA64.tar.Z
AIX v5.3 Power	pam_CA_eta-1.1.AIX.tar.Z
Solaris Sparc	pam_CA_eta-1.1.Solaris.tar.Z
Solaris Intel	pam_CA_eta-1.1.SolarisIntel.tar.Z
Linux x86	pam_CA_eta-1.1.Linux.tar.gz
Linux s390	pam_CA_eta-1.1.LinuxS390.tar.gz

2. Übertragen Sie die gewählte Paketdatei in einen temporären Ordner (/tmp) auf dem UNIX-Server mithilfe von FTP im binären Modus oder mit einem anderen Dateiübertragungstool, das binäre Dateien unterstützt. Eine Übertragungssitzung könnte beispielsweise folgendermaßen angezeigt werden:

```
W:\Pam>ftp user01
Connected to user01.company.com.
220 user01 FTP server (Version 1.2.3.4) ready.
User (user01.company.com:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> bin
200 Type set to I.
ftp> put pam_CA_eta-1.1.HPUX.tar.Z
200 PORT command successful.
150 Opening BINARY mode data connection for pam_CA_eta-1.1.HPUX.tar.Z.
226 Transfer complete.
ftp: 117562 bytes sent in 0,09Seconds 1306,24Kbytes/sec.
ftp> quit
```

3. Melden Sie sich als Root-Benutzer auf dem UNIX-Server an, und extrahieren Sie die Paketdatei:

   ```
   # cd /tmp
   # zcat pam_CA_eta-1.1.<platform>.tar.Z | tar -xf -
   ```

   Verwenden Sie unter Linux den folgenden Befehl:

   ```
   # tar -xzf pam_CA_eta-1.1.<platform-hardware>.tar.gz
   ```

4. Kopieren Sie die Konfigurations- und TLS-Dateien in den Standardkonfigurationsordner:

   ```
   # cd pam_CA_eta-1.1
   # mv pam_CA_eta /etc
   ```

5. Kopieren Sie das pam_CA_eta-Modul in den Sicherheits-Bibliotheks-Ordner:

   Verwenden Sie unter AIX den folgenden Befehl:

   ```
   # cp -p pam_CA_eta.o /usr/lib/security/
   ```

   Verwenden Sie unter HP-UX den folgenden Befehl:

   ```
   # cp -p libpam_CA_eta.1 /usr/lib/security/
   ```

   Verwenden Sie unter HP-UX Itanium2 den folgenden Befehl:

   ```
   # cp -p libpam_CA_eta.1 /usr/lib/security/hpux32
   ```

   Verwenden Sie unter Linux i386 oder s390 den folgenden Befehl:

   ```
   # cp -p pam_CA_eta.so /lib/security/
   ```

   Verwenden Sie unter Solaris Sparc oder Intel den folgenden Befehl:

   ```
   # cp -p pam_CA_eta.so /usr/lib/security/
   ```

6. (Optional) Kopieren Sie die Test-Programme:

   ```
   # cp -p test_* /etc/pam_CA_eta
   # cp -p pam_test* (/usr)/lib/security/
   ```

Weitere Informationen:

Fehlerbehebung bei der UNIX-Kennwortsynchronisierung (siehe Seite 155)

Aktualisieren des Endpunkts in der Benutzerkonsole

Aktualisieren Sie den Endpunkt in der Benutzerkonsole, um anzuzeigen, dass der Agent installiert wird.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole an.
2. Klicken Sie auf "Endpunkte", "Manage Endpoints" (Endpunkte verwalten), "Endpunkt ändern".
3. Suchen Sie nach dem Endpunkt, auf dem der Agent installiert ist.
4. Klicken Sie auf die Registerkarte "Endpunkteinstellungen".
5. Aktivieren Sie das Kontrollkästchen "Agent für die Kennwortsynchronisierung ist installiert".

Aktivieren einer Umgebung für die Kennwortsynchronisierung

Nachdem Sie den Agenten für die Kennwortsynchronisierung installiert haben, aktivieren Sie die Umgebung für den Eingang von Kennwortänderungen, die auf den Endpunkten vorgenommen wurden. Der Administrator benötigt für diese Aufgabe Zugriff auf die Management-Konsole und CA Directory, um die Umgebung so einzurichten, dass diese Änderungen akzeptiert werden.

Gehen Sie wie folgt vor:

1. Für neue Benutzer verwenden Sie die Management-Konsole folgendermaßen:
   a. Wählen Sie die Umgebung aus.
   b. Klicken Sie auf "Advanced Settings" (Erweiterte Einstellungen), "Provisioning" (Bereitstellung).
   c. Aktivieren Sie das Kontrollkästchen "Enable Password Changes from Endpoint Accounts" (Kennwortänderungen auf Endpunktkonten aktivieren).
2. Legen Sie das Attribut "eTPropagatePassword" in CA Directory für vorhandene Benutzer auf "1" fest.

Konfigurieren der UNIX-Kennwortsynchronisierungs-Funktion

Bei der Konfiguration der UNIX-Kennwortsynchronisierungs-Funktion müssen Einstellungsparameter in den folgenden Dateien festgelegt werden:

- /etc/pam_CA_eta/pam_CA_eta.conf
- /etc/pam.conf

Wichtig! Da das Kennwort von Benutzern mit hoher Berechtigungsstufe in der pam_CA_eta.conf-Konfigurationsdatei gespeichert wird, darf nur das Root-Konto Lesezugriff auf diese Datei haben. Beachten Sie, dass die Dateieinstellungen in der Paketdatei owner=root und mode=500 umfassen und dass der -p-Schalter des cp-Befehls sie während der Installation beibehält.

Konfigurieren der pam_CA_eta.conf-Datei

Gehen Sie folgendermaßen vor, um die pam_CA_eta.conf-Datei zu konfigurieren.

So konfigurieren Sie die pam_CA_eta.conf-Datei

1. Navigieren Sie zum Ordner "/etc/pam_CA_eta.
2. Bearbeiten Sie die Datei "pam_CA_eta.conf". Diese Konfigurationsdatei enthält die eigene Dokumentation.

```
#
#   CA - CA IdentityMinder
#
#   pam_CA_eta.conf
#
#   Configuration file for the Unix PAM password module "pam_CA_eta"
#

# keyword: server
# description: the CA IdentityMinder LDAP server primary and optional alternate
server hostname
# value: a valid hostname and an optional server
# default: no default
server ETA_SERVER ALT_SERVER

#

# keyword: port
# description: the numeric TCP/IP port number of the CA IdentityMinder LDAP server
# value: a valid TCP/IP port number
# default: 20390
# port 20390


# keyword: use-tls
# description: does it use the secured LDAP over TLS protocol ?
# value: yes or no
# default: yes
# use-tls yes
```

```
# keyword: time-limit
# description: the maximum time in seconds to wait for the end of an LDAP operation.
# value: a numeric value of seconds
# default: 300
# time-limit 300

# keyword: remote-server
# description: identifies whether on premise or cloud Identity Manager
#              server is used.
#              Cloud based server is accessed by proxying the requests
#              through the on-premise CS, requiring use of remote-server
#              set to 'yes'.
# value: yes or no
# default: no
# remote-server no

# keyword: size-limit
# description: the maximum number of entries returned by the CA IdentityMinder
server
# value: a numeric value
# default: 100
# size-limit 100


# keyword: root
# description: the root DN of the CA IdentityMinder server
# value: a valid DN string
# default: dc=eta
# root dc=eta


# keyword: domain
# description: the name of the CA IdentityMinder domain
# value: a string
# default: im
# domain    im


# keyword: user
# description: the CA IdentityMinder Global User name used to bind to the CA
IdentityMinder server
# value: a valid Global User name string
# default: etaadmin
# user etaadmin


# keyword: password
# description: the clear-text password of the "binding" CA IdentityMinder Global
User
# value: the password of the above Global User
# default: no default
password SECRET
```

```
# keyword: directory-type
# description: the CA IdentityMinder Unix Endpoint type of this Unix server
# value: ETC or NIS
# default: ETC
# endpoint-type ETC


# keyword: endpoint-name
# description: the CA IdentityMinder Unix Endpoint name of this Unix server
# value: a valid Unix Endpoint name string
# default:
# ETC: the result of the "hostname" command (ie: gethostname() system call)
# NIS: "domain [hostname]" where "domain" is the result of the "domainname" command
#  (ie: getdomainname() system call) and "hostname" the result of the "hostname"
#    command (ie: gethostname() system call)
# endpoint-name dirname


# keyword: tls-cacert-file
# description: the name of the CA IdentityMinder CA certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/et2_cacert.pem
# tls-cacert-file /etc/pam_CA_eta/et2_cacert.pem


# keyword: tls-cert-file
# description: the name of the CA IdentityMinder client certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientcert.pem
# tls-cert-file /etc/pam_CA_eta/eta2_clientcert.pem


# keyword: tls-key-file
# description: the name of the CA IdentityMinder client private key file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientkey.pem
# tls-key-file /etc/pam_CA_eta/eta2_clientkey.pem


# keyword: tls-random-file
# description: the name of the "pseudo random number generator" seed file
# value: a valid full path file name
# default: /etc/pam_CA_eta/prng_seed
# tls-random-file /etc/pam_CA_eta/prng_seed


# keyword: use-status
# description: this module will exit with a non-zero status code in case of failure.
# value: yes or no
# default: no
# use-status no
```

```
# keyword: verbose
# description: this module will display informational or error messages to the
user.
# value: yes or no
# default: yes
# verbose yes
```

Hinweis: Die Server-, Domänen- und Kennwortparameter haben keinen Standardwert und müssen aktualisiert werden.

Konfigurieren der pam.conf-Datei

Die Datei "/etc/pam.conf" ist die hauptsächliche PAM-Konfigurationsdatei. Sie müssen die Datei bearbeiten und eine Zeile im Kennwort-Service-Stack einfügen. Auf einigen Linux-Systemen wird die Datei "pam.conf" durch "/etc/pam.d" ersetzt, sodass Sie die Datei "/etc/pam.d/system-auth" bearbeiten müssen.

So konfigurieren Sie die Datei "pam.conf"

1. Navigieren Sie zum Verzeichnis "/etc" oder "/etc/pam.d", wenn Sie das PAM-Modul auf einem geeigneten Linux-System konfigurieren.
2. Bearbeiten Sie die Datei "pam.conf", und fügen Sie eine Zeile für die Kennwortsynchronisierung im Kennwort-Service-Stack ein. Die nachfolgenden Beispiele zeigen Plattform-spezifische Konfigurationen:

   passwd password required /usr/lib/security/pam_unix.so

   passwd password optional /usr/lib/security/pam_CA_eta.so

3. (Optional) Sie können die folgenden optionalen Parameter in der Zeile für das pam_CA_eta-Modul hinzufügen:

   config=/path/file

   Zeigt den Speicherort einer alternativen Konfigurationsdatei an.

   Syslog

   Sendet Fehler und informative Meldungen an den lokalen Syslog-Service.

   trace

   Generiert eine Ablaufverfolgungsdatei für jeden Kennwortaktualisierungsvorgang. Die Ablaufverfolgungsdateien werden "/tmp/pam_CA_eta-trace.<nnnn>" genannt, wobei <nnnn> die PID-Anzahl des Kennwortprozesses ist.

4. Implementieren Sie die folgenden Plattform-spezifischen Konfigurationsänderungen:

   Fügen Sie für AIX-Systeme die folgenden Zeilen am Ende der Datei "/etc/pam.conf" hinzu:

   ```
   #
   # CA IdentityMinder Unix Password Synchronization
   #
   login   password  optional    /usr/lib/security/pam_CA_eta.so syslog
   passwd  password  optional    /usr/lib/security/pam_CA_eta.so syslog
   rlogin  password  optional    /usr/lib/security/pam_CA_eta.so syslog
   su      password  optional    /usr/lib/security/pam_CA_eta.so syslog
   telnet  password  optional    /usr/lib/security/pam_CA_eta.so syslog
   sshd    password  optional    /usr/lib/security/pam_CA_eta.so syslog
   OTHER   password  optional    /usr/lib/security/pam_CA_eta.so syslog
   ```

   Fügen Sie für HP-UX-Systeme die folgenden Zeilen am Ende der Datei "/etc/pam.conf" hinzu:

   ```
   #
   # CA IdentityMinder Unix Password Synchronization
   #
   login    password optional    /usr/lib/security/libpam_CA_eta.1 syslog
   passwd   password optional    /usr/lib/security/libpam_CA_eta.1 syslog
   dtlogin  password optional    /usr/lib/security/libpam_CA_eta.1 syslog
   dtaction password optional    /usr/lib/security/libpam_CA_eta.1 syslog
   OTHER    password optional    /usr/lib/security/libpam_CA_eta.1 syslog
   ```

   Fügen Sie für HP-UX Itanium2 die folgenden Zeilen am Ende der Datei "/etc/pam.conf" hinzu:

   ```
   #
   # CA IdentityMinder Unix Password Synchronization
   ```

```
#
login    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
passwd   password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
dtlogin  password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
dtaction password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
OTHER    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
```

Fügen Sie für Sun Solaris-Systeme die Zeile "pam_CA_eta" nach der vorhandenen Zeile "pam_unix" hinzu:

```
#
# Password management
#
other   password required       /usr/lib/security/pam_unix.so.1
other   password optional       /usr/lib/security/pam_CA_eta.so syslog
```

Fügen Sie für Linux-Systeme die Zeile "pam_CA_eta" zwischen den vorhandenen Zeilen "pam_cracklib" und "pam_unix" hinzu:

```
password    required     /lib/security/pam_cracklib.so retry=3 type=
password    optional     /lib/security/pam_CA_eta.so syslog
password   sufficient  /lib/security/pam_unix.so nullok use_authtok md5 shadow
password    required     /lib/security/pam_deny.so
```

5. Bearbeiten Sie für AIX-Systeme die Datei "/etc/security/login.cfg", und legen Sie auth_type = PAM_AUTH fest. Dadurch wird das PAM-Framework aktiviert, das nicht standardmäßig aktiviert ist. Dies ist eine Laufzeiteinstellung, sodass Sie das System nicht neu starten müssen, damit die Einstellung wirksam wird.

Fehlerbehebung bei der UNIX-Kennwortsynchronisierung

Für die Fehlerbehebung im Zusammenhang mit der UNIX PAM-Funktion können Sie Syslog und Ablaufverfolgungsmeldungen verwenden und die Konfiguration, die LDAP/TLS-Verbindung, die Kennwortsynchronisierung und das PAM-Framework testen.

Weitere Informationen:

Aktivieren von Syslog-Meldungen (siehe Seite 156)
Aktivieren von Verfolgungsmeldungen (siehe Seite 156)

Aktivieren von Syslog-Meldungen

Fügen Sie den Syslog-Parameter in die Zeile "pam_CA_eta" in der Datei "/etc/pam.conf" hinzu, damit das Modul "pam_CA_eta" Informationen und Fehlermeldungen generiert. Wenn die Protokollierungsoption verwendet wird, sieht der UNIX-Administrator jedes Mal, wenn ein UNIX-Konto das Kennwort ändert, Informationsmeldungen in den Syslog-Dateien. Diese Meldungen sollten ausreichende Informationen zur Diagnose von einfachen Problemen zur Verfügung stellen.

Sie können diese Option auf Produktionssystemen dauerhaft festlegen, da sie nicht viel mehr Ressourcen benötigt als bei der Ausführung im unbeaufsichtigten Modus.

Aktivieren von Verfolgungsmeldungen

Wenn die Syslog-Meldungen nicht genügend Informationen enthalten, kann der Verfolgungsmodus weitere Details bereitstellen. Für jeden Kennwortaktualisierungsvorgang generiert das Verfolgungsmodul eine Datei mit dem Namen /tmp/pam_CA_eta-trace.<nnnn>" (wobei <nnnn> die PID des Kennwortprozesses ist), die einen Eintrag für die meisten der Funktionsaufrufe, die vom Modul verwendet werden, und der Daten, die von diesen Funktionen verwendet oder zurückgegeben werden, enthält.

Das Root-Konto hat zwar nur Lesezugriff auf die Verfolgungsdateien, aber diese Dateien enthalten die neuen Klartext-Kennwörter. Aus diesem Grund sollte dieser Parameter auf einem Produktionssystem nicht dauerhaft verwendet werden.

Testen der Konfigurationsdatei

Sie können das test_config-Tool verwenden, das sich im Verzeichnis "/etc/pam_CA_eta" befindet, um die Konfigurationsdatei zu überprüfen. Richten Sie als Erstes die Ordnerstruktur wie folgt ein:

1. Verschieben Sie den Ordner "pam_CA_eta" unter den Ordner "/etc".
2. Kopieren Sie alles unter "pam_CA_eta-1.1" nach "/etc/pam_CA_eta".

Beispiel für eine Befehlszeileneingabe:

```
/etc/pam_CA_eta/test_config [config=/path/to/config_file]
```

Beispiel für eine Sitzung:

```
./test_config [config=/path/to/config_file]
# ./test_config
./test_config: succeeded
Trace file is /tmp/test_config-trace.1274
```

Wie die Befehlsausgabe zeigt, wurde eine Verfolgungsdatei generiert, die alle Details der Konfigurationsdateianalyse enthält.

Anzeigen des CAM-Service

Gehen Sie folgendermaßen vor, um herauszufinden, wer den Service gestartet hat.

So zeigen Sie den CAM-Service an

1. Melden Sie sich bei Ihrem UNIX-Rechner als Root-Benutzer mit dem Telnet- oder SSH-Client an.
2. Geben Sie den folgenden UNIX-Befehl aus:

   ```
   ps -ef | grep cam
   ```

   Die daraufhin angezeigten Zeichenfolgen entsprechen in etwa Folgendem:

   ```
   root 13822        1 11 11:30:12 ?   0:00 cam
   root 13843 13753  3 11:56:31 pts/5  0:00 grep cam
   ```

Hinweis: Wenn der Root-Benutzer des Systems die Services nicht startet, werden sie als gestartet angezeigt, aber Sie können sie nicht verwenden. CA IdentityMinder gibt die folgende Meldung aus: "Permission denied: user must be root" (Berechtigung verweigert: Benutzer muss ein Root-Benutzer sein).

Testen der LDAP/TLS-Verbindung

Sie können das test_ldap-Tool verwenden, das sich im Verzeichnis "/etc/pam_CA_eta" befindet, um die Verbindung mit dem Bereitstellungsserver (mithilfe der Konfigurationsdateiparameter) zu überprüfen. Beispiel für eine Befehlszeileneingabe:

```
/etc/pam_CA_eta/test_ldap [config=/path/to/config_file]
```

Beispiel für eine Sitzung:

```
./test_ldap [config=/path/to/config_file]
# ./test_ldap: succeeded
Trace file is /tmp/test_ldap-trace.1277
```

Wie die Befehlsausgabe zeigt, wurde eine Verfolgungsdatei generiert, die alle Details zur Konfigurationsdateianalyse und zur Verbindung mit dem Bereitstellungsserver enthält.

Testen der Kennwortsynchronisierung

Sie können das test_sync-Tool verwenden, das sich im Ordner "/etc/pam_CA_eta" befindet, um zu überprüfen, ob die Kennwortaktualisierung eines lokalen Kontos vom Bereitstellungsserver effektiv übertragen wird. Beispiel für eine Befehlszeileneingabe:

```
/etc/pam_CA_eta/test_sync <Benutzer> <Kennwort> [config=/path/to/config_file]
```

Beispiel für eine Sitzung:

```
# /etc/pam_CA_eta/test_sync pam002 newpass1234
CA IdentityMinder password synchronization started.
:ETA_S_0245<MGU>, Global User 'pam002' and associated account passwords updated
successfully: (accounts updated: 2, unchanged: 0, failures: 0)
CA IdentityMinder password synchronization succeeded.
/etc/pam_CA_eta/test_sync: succeeded
Trace file is /tmp/test_sync-trace.2244
```

Wie die Befehlsausgabe zeigt, wurde eine Verfolgungsdatei generiert, die alle Details zur Konfigurationsdateianalyse, zur Verbindung mit dem Bereitstellungsserver und zur Aktualisierung des Kontos enthält.

Wenn der ausführliche Modus verwendet wird (indem der Standardparameter (ja) für den ausführlichen Modus in der Konfigurationsdatei verwendet wird), liefert der Befehl informative und potenzielle Fehlermeldungen über die Kennwortpropagierung.

Testen des PAM-Frameworks

Eine PAM-Testbibliothek ist verfügbar, mit der überprüft werden kann, ob die Kennwortänderungen vom PAM-Framework richtig erkannt werden.

So testen Sie das PAM-Framework

1. Kopieren Sie die Datei "pam_test" in den Ordner "/usr/lib/security(/hpux32)".
2. Fügen Sie eine Zeile für die Kennwortklasse für die pam_test-Bibliothek ohne Parameter hinzu.

   Beispiel für Solaris:

   ```
   other password optional /usr/lib/security/pam_test
   ```

3. Geben Sie einen passwd-Befehl für einen Testbenutzer aus, und suchen Sie dann nach der markierten Zeile "pam_test[<pid>]" in der Syslog-Datei.

   Die Befehlsausgabe zeigt den Namen der generierten Verfolgungsdatei, zum Beispiel:

   ```
   pam_test[1417]: Succeeded, trace file is /tmp/pam_test-trace.1417
   ```

Kennwortsynchronisierung auf OS400

Mit dem Agenten für die Kennwortsynchronisierung können Kennwortänderungen, die auf dem OS/400-Endpunktsystem vorgenommen wurden, an Ihre anderen von CA IdentityMinder verwalteten Konten propagiert werden. Der Agent für die Kennwortsynchronisierung funktioniert folgendermaßen:

1. Installieren Sie den Agenten auf dem OS/400-Endpunktsystem, und führen Sie ihn aus.

   Das Programm wird im Rahmen der Installation beim OS/400-System registriert, sodass der Agent, wenn Benutzer ihre Kennwörter ändern, die Kennwortänderungen an den Bereitstellungsserver weiterleitet.

2. Der Bereitstellungsserver propagiert die Kennwortänderung an die zugeordneten Konten.

   Kennwortänderungen, die mit einem Befehl zur Änderung des Kennworts (CHGPWD) oder einer API zur Änderung des Kennworts (QSYCHGPW) initiiert werden, gehen beim Agenten ein.

3. Der Agent protokolliert in einer Protokolldatei unter PWDSYNCH/LOG, ob der Vorgang erfolgreich war oder fehlgeschlagen ist.

Der Agent für die Kennwortsynchronisierung wird auf den folgenden Plattformen unterstützt:

- OS400 V5R2
- OS400 V5R3
- OS400 V5R4

So installieren Sie den Agenten für die Kennwortsynchronisierung

1. Suchen Sie nach den Installationsdatenträgern für die Bereitstellungskomponenten.
2. Führen Sie das Installationsprogramm des Agenten für die Kennwortsynchronisierung oder OS/400 unter "\Agent" aus.
3. Folgen Sie den Bildschirmanweisungen, um die Installation abzuschließen.

   Hinweis: Die Installationsanweisungen im Endpunkt-Agent-Software-Link finden Sie in den folgenden Abschnitten.

Installieren des OS400-Kennwortsynchronisierungs-Agenten

Sie müssen über *ADDOBJ-Berechtigungen verfügen, und die folgenden Anforderungen müssen erfüllt sein, damit der Agent Benachrichtigungen über Kennwortänderungen erhält:

- Systemwert QPWDVLDPGM muss auf *REGFAC festgelegt werden
- Programm muss mit dem Befehl WRKREGINF EXITPNT(QIBM_QSY_VLD_PASSWRD) registriert werden
- Die Umgebung muss so eingerichtet sein, dass Kennwortänderungen aus Endpunktkonten akzeptiert werden. Diese Funktion wird von einem Administrator mit Zugriff auf die Management-Konsole aktiviert.

Der Agent wird nur initiiert, wenn eine Kennwortänderung vorgenommen wird. Um das Kennwort zu ändern, geben Sie den CHGPWD-Befehl aus.

Hinweis: Der globale Benutzer muss für die Kennwortsynchronisierung gekennzeichnet werden.

Auf der iSeries

1. Melden Sie sich als Benutzer mit *ALLOBJ- und *SECADM-Berechtigungen an (zum Beispiel QSECOFR).
2. Erstellen Sie einen Benutzer mit den Namen PWDSYNCH:

   ```
   CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
   ```

   Hinweis: Als Sicherheitsmaßnahme wird der Benutzer mit abgelaufenem Kennwort erstellt.

3. Erstellen Sie eine Speicherdatei, um das Installationspaket in einer Bibliothek Ihrer Wahl zu speichern (zum Beispiel MYLIB):

   ```
   CRTSAVF MYLIB/PWDSYNCH
   ```

4. Verwenden Sie auf dem Windows-Rechner mit der Speicherdatei FTP, um die Speicherdatei an die iSeries zu übertragen:

   ```
   ftp <Hostname>
   binär
   cd MYLIB
   put PWDSYNCH.FILE
   ```

5. Extrahieren Sie auf der iSeries das Programm aus der Speicherdatei:

   ```
   RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
   ```

   Mit diesem Befehl wird der Synchronisierungsagent in die PWDSYNCH-Bibliothek extrahiert und installiert.

6. Überprüfen Sie die Installation:

   ```
   DSPLIB PWDSYNCH
   ```

   Die folgenden Objekte sollten angezeigt werden:

Objekt	Typ	Attribut
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

7. Richten Sie die iSeries so ein, dass PWDSYNCH als Kennwortvalidierungs-Exit-Programm verwendet wird:

   ```
   CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
   ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
   PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
   ```

8. Geben Sie auf der iSeries die Verbindungsparameter für Ihren CA IAM-Connector-Server an:

   ```
   EDTF FILE(PWDSYNCH/CONFIG)
   ```

Installieren des OS400-Kennwortsynchronisierungs-Agenten

Sie müssen über *ADDOBJ-Berechtigungen verfügen, und die folgenden Anforderungen müssen erfüllt sein, damit der Agent Benachrichtigungen über Kennwortänderungen erhält:

- Systemwert QPWDVLDPGM muss auf *REGFAC festgelegt werden
- Programm muss mit dem Befehl WRKREGINF EXITPNT(QIBM_QSY_VLD_PASSWRD) registriert werden
- Die Umgebung muss so eingerichtet sein, dass Kennwortänderungen aus Endpunktkonten akzeptiert werden. Diese Funktion wird von einem Administrator mit Zugriff auf die Management-Konsole aktiviert.

Der Agent wird nur initiiert, wenn eine Kennwortänderung vorgenommen wird. Um das Kennwort zu ändern, geben Sie den CHGPWD-Befehl aus.

Hinweis: Der globale Benutzer muss für die Kennwortsynchronisierung gekennzeichnet werden.

Auf der iSeries

1. Melden Sie sich als Benutzer mit *ALLOBJ- und *SECADM-Berechtigungen an (zum Beispiel QSECOFR).
2. Erstellen Sie einen Benutzer mit den Namen PWDSYNCH:

   ```
   CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
   ```

   Hinweis: Als Sicherheitsmaßnahme wird der Benutzer mit abgelaufenem Kennwort erstellt.
3. Erstellen Sie eine Speicherdatei, um das Installationspaket in einer Bibliothek Ihrer Wahl zu speichern (zum Beispiel MYLIB):

   ```
   CRTSAVF MYLIB/PWDSYNCH
   ```
4. Verwenden Sie auf dem Windows-Rechner mit der Speicherdatei FTP, um die Speicherdatei an die iSeries zu übertragen:

   ```
   ftp <Hostname>
   binär
   cd MYLIB
   put PWDSYNCH.FILE
   ```
5. Extrahieren Sie auf der iSeries das Programm aus der Speicherdatei:

   ```
   RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
   ```

   Mit diesem Befehl wird der Synchronisierungsagent in die PWDSYNCH-Bibliothek extrahiert und installiert.

6. Überprüfen Sie die Installation:

   ```
   DSPLIB PWDSYNCH
   ```

   Die folgenden Objekte sollten angezeigt werden:

Objekt	Typ	Attribut
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

7. Richten Sie die iSeries so ein, dass PWDSYNCH als Kennwortvalidierungs-Exit-Programm verwendet wird:

   ```
   CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
   ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
   PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
   ```

8. Geben Sie auf der iSeries die Verbindungsparameter für Ihren CA IAM-Connector-Server (CA IAM CS) an:

   ```
   EDTF FILE(PWDSYNCH/CONFIG)
   ```

Aktualisieren des Endpunkts in der Benutzerkonsole

Aktualisieren Sie den Endpunkt in der Benutzerkonsole, um anzuzeigen, dass der Agent installiert wird.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole an.
2. Klicken Sie auf "Endpunkte", "Manage Endpoints" (Endpunkte verwalten), "Endpunkt ändern".
3. Suchen Sie nach dem Endpunkt, auf dem der Agent installiert ist.
4. Klicken Sie auf die Registerkarte "Endpunkteinstellungen".
5. Aktivieren Sie das Kontrollkästchen "Agent für die Kennwortsynchronisierung ist installiert".

Aktivieren einer Umgebung für die Kennwortsynchronisierung

Nachdem Sie den Agenten für die Kennwortsynchronisierung installiert haben, aktivieren Sie die Umgebung für den Eingang von Kennwortänderungen, die auf den Endpunkten vorgenommen wurden. Der Administrator benötigt für diese Aufgabe Zugriff auf die Management-Konsole und CA Directory, um die Umgebung so einzurichten, dass diese Änderungen akzeptiert werden.

Gehen Sie wie folgt vor:

1. Für neue Benutzer verwenden Sie die Management-Konsole folgendermaßen:
   a. Wählen Sie die Umgebung aus.
   b. Klicken Sie auf "Advanced Settings" (Erweiterte Einstellungen), "Provisioning" (Bereitstellung).
   c. Aktivieren Sie das Kontrollkästchen "Enable Password Changes from Endpoint Accounts" (Kennwortänderungen auf Endpunktkonten aktivieren).
2. Legen Sie das Attribut "eTPropagatePassword" in CA Directory für vorhandene Benutzer auf "1" fest.

SSL-Konfiguration

SSL wird verwendet, um die Kommunikation zwischen dem Synchronisierungs-Agenten und dem Bereitstellungsserver zu verschlüsseln. Dies ist für den Synchronisierungs-Agenten wichtig, weil SSL Kennwörter über das gesamte Netzwerk hinweg sendet. Es wird empfohlen, dass SSL immer verwendet wird.

Der Synchronisierungs-Agent muss dem Zertifikat des Bereitstellungsservers vertrauen, um eine Verbindung mit SSL herzustellen. Deswegen muss das Zertifikat auf dem iSeries-Rechner installiert und so konfiguriert werden, dass der Synchronisierungs-Agent dem Zertifikat vertraut. Diese Aufgaben werden vom Digital Certificate Manager, einer optionalen Komponente von OS/400, ausgeführt. Folgen Sie den entsprechenden Anweisungen in der OS/400-Dokumentation, um den Digital Certificate Manager zu installieren und einzurichten.

Installieren des Zertifikats für den Bereitstellungsserver

Die folgenden Betriebssystemkomponenten müssen auf Ihrem iSeries-Rechner installiert sein, damit SSL verwendet werden kann:

- Cryptographic Access Provider, lizenziertes Programm (5722-AC3)
- Digital Certificate Manager (Option 34 von OS/400)
- IBM-HTTP-Server für iSeries (5722-DG1)

Auf der iSeries

1. Laden Sie das Zertifikat des Bereitstellungsservers vom Bereitstellungsserver-Computer auf die iSeries hoch. Das Zertifikat befindet sich unter:

   ```
   C:\Programme\CA\Identity Manager\Provisioning
   Server\Data\Tls\server\et2_cacert.pem
   ```

2. Melden Sie sich beim DCM an.

   Navigieren Sie mithilfe eines Webbrowsers zu http://<Hostname>:2001. Wenn Sie dazu aufgefordert werden, melden Sie sich als QSECOFR an, und klicken Sie auf den Digital Certificate Manager-Link.

3. Arbeiten Sie mit dem *SYSTEM-Zertifikatspeicher.

   Klicken Sie auf die Schaltfläche "Wählen Sie einen Zertifikatspeicher aus", und wählen Sie den *SYSTEM-Zertifikatspeicher aus. Wenn dieser Speicher nicht vorhanden ist, erstellen Sie einen neuen Speicher mit dem Namen *SYSTEM, und geben Sie dann das Kennwort für den Zertifikatspeicher ein.

4. Importieren Sie das Zertifikat als CA Zertifikat mithilfe des DCM.

   Klicken Sie auf "Zertifikate verwalten", "Zertifikat importieren", und wählen Sie die Option "Certificate Authority (CA)" (Zertifizierungsstelle) aus. Geben Sie dann den Dateinamen des Zertifikats des Bereitstellungsservers ein. (Das Zertifikat befindet sich in dem Ordner, in den Sie es in Schritt 1 hochgeladen haben.) Geben Sie die Bezeichnung "Bereitstellungsserver" für das Zertifikat ein.

   Das Importieren des Zertifikats ist abgeschlossen.

5. Nachdem Sie das CA-Zertifikat in den *SYSTEM-Schlüsselspeicher auf dem Endpunkt importiert haben, müssen Sie sicherstellen, dass der IBM Directory-Client QIBM_GLD_DIRSRV_CLIENT auf den *SYSTEM-Schlüsselspeicher zugreifen kann. Andernfalls schlägt der SSL-Initialisierungsaufruf des PSA fehl.

6. Konfigurieren Sie die Verzeichnisdienste-Client-Anwendung so, dass das Zertifikat des Bereitstellungsservers als vertrauensvoll eingestuft wird, indem Sie "Manage Applications" (Anwendungen verwalten) und "Define CA trust list" (Vertrauensliste der Zertifizierungsstelle definieren) öffnen und "Directory Services Client" auswählen.

   Das Zertifikat des Bereitstellungsservers sollte hier aufgeführt sein, wenn es in Schritt 4 richtig importiert wurde.

   Klicken Sie für das Zertifikat des Bereitstellungsservers auf "Vertrauenswürdig", und klicken Sie am Ende der Liste auf "OK".

7. Erteilen Sie den SSL-Dateien die Leseberechtigung PUBLIC, und gewähren Sie Lesezugriff auf den *SYSTEM-Zertifikatspeicher:

   ```
   (/QIBM/userdata/ICSS/Cert/Server/default.kdb)
   ```

   Erteilen Sie dem übergeordneten Ordner die Berechtigungen "Lesen" und "Ausführen".

   ```
   (/QIBM/userdata/ICCS/Cert/Server)
   ```

   Hinweis: Die Übernahme der PWDSYNCH-Berechtigung von Benutzern funktioniert im Dateisystem mit dem /-Zeichen nicht, sodass Zugriff für alle Benutzer erteilt werden muss.

Deinstallieren des Agenten für die Kennwortsynchronisierung

Wenn Sie den Agenten für die Kennwortsynchronisierung deinstallieren müssen, gehen Sie folgendermaßen vor.

Über den Kennwortvalidierungs-Exit-Point

1. Entfernen Sie PWDSYNCH:

   ```
   RMVEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
   ```

2. Löschen Sie die Bibliothek des Synchronisierungs-Agenten:

   ```
   DLTLIB PWDSYNCH
   ```

3. Löschen Sie den PWDSYNCH-Benutzer:

   ```
   DLTUSRPRF PWDSYNCH
   ```

4. Entfernen Sie das Zertifikat des Bereitstellungsservers, indem Sie den SSL-Anweisungen folgen, um sich beim DCM anzumelden und mit dem *SYSTEM-Zertifikatspeicher zu arbeiten:

   Klicken Sie auf "Zertifikate verwalten", "Zertifikat löschen", und wählen Sie "Certificate Authority (CA)" (Zertifizierungsstelle) aus.

   Wählen Sie das Zertifikat "Bereitstellungsserver", und klicken Sie auf "Löschen".

Parameter für Kennwort-Agent unter OS/400 muss richtig gesetzt werden

Der Wert des Parameters "pwd_case_action" muss für eine ordnungsgemäße Funktion richtig gesetzt werden. Korrekte Werte sind:

- pwd_case_action = pwd_case_unchanged
- pwd_case_action = pwd_to_uppercase
- pwd_case_action = pwd_to_lowercase

Bei pwd_case_action = [ungültiger Wert] wird die Großschreibung des Kennworts erzwungen.

Hinweis: Beachten Sie den QPWDLVL-Systemwert (Kennwortstufe), wenn Sie den Agenten für die Kennwortsynchronisierung konfigurieren.

- Wenn QPWDLVL auf dem AS400-System auf 0 (Standardwert) festgelegt ist, werden Kennwörter mit einer Länge von 1 bis 10 Großbuchstaben unterstützt.
- Wenn QPWDLVL auf 2 oder 3 festgelegt ist, werden Kennwörter mit einer Länge von 1 bis 128 Zeichen mit Groß- und Kleinbuchstaben unterstützt.

In der Standardeinstellung propagiert der PSA das unveränderte Kennwort an den Bereitstellungsserver. Sie können jedoch unabhängig vom QPWDLVL-Wert erzwingen, dass der PSA Kennwörter mit Groß- oder Kleinbuchstaben propagiert, indem Sie "pwd_case_action" auf "pwd_to_uppercase" bzw. "pwd_to_lowercase" festlegen.

Kapitel 7: Gruppen

Sie können einige Typen von Gruppen oder eine Kombination dieser Typen erstellen:

- Statische Gruppe: Eine Liste von Benutzern, die interaktiv hinzugefügt werden
- Dynamische Gruppe: Benutzer gehören zu einer Gruppe, wenn sie einer LDAP-Abfrage entsprechen (Erfordert ein LDAP-Verzeichnis als Benutzerspeicher)

  Hinweis: Das Feld "Dynamische Gruppenabfrage" wird nicht in die Aufgabe "Gruppe erstellen" oder in andere Gruppenaufgaben eingeschlossen, auch wenn dieses Feld im directory.xml für eine Gruppe vorhanden ist. Das Feld "Dynamische Gruppenabfrage" schließen Sie in der Aufgabe ein, indem Sie das verknüpfte Profilfenster bearbeiten.
- Verschachtelte Gruppe: Eine Gruppe, die andere Gruppen enthält (Erfordert ein LDAP-Verzeichnis als Benutzerspeicher)

Hinweis: Verwenden Sie die Registerkarte "Gruppen" für das Benutzerobjekt, um die statischen, dynamischen und verschachtelten Gruppen anzuzeigen, zu denen ein Benutzer gehört. Diese Registerkarte wird standardmäßig in den Aufgaben zur Ansicht und zum Ändern von Benutzern angezeigt.

Dieses Kapitel enthält folgende Themen:

Erstellen einer statischen Gruppe (siehe Seite 169)
Erstellen einer dynamischen Gruppe (siehe Seite 170)
Parameter für dynamische Gruppenabfragen (siehe Seite 171)
Erstellen von verschachtelten Gruppen (siehe Seite 173)
Beispiel für statische, dynamische und verschachtelte Gruppen (siehe Seite 175)
Gruppenadministratoren (siehe Seite 176)

Erstellen einer statischen Gruppe

Sie können eine Sammlung von Benutzern einer *statischen Gruppe* zuordnen. Sie können die statische Gruppe verwalten, indem Sie einzelne Benutzer zur Liste der Gruppenmitglieder hinzufügen oder daraus entfernen. Verwenden Sie die Registerkarte "Mitgliedschaft", die sich standardmäßig in den Aufgaben zum Anzeigen und Ändern von Gruppen befindet, um die Liste der Mitglieder einer Gruppe anzuzeigen.

Hinweis: Die Registerkarte "Mitgliedschaft" zeigt nur die Mitglieder an, die explizit zur Gruppe hinzugefügt wurden. Sie zeigt keine Mitglieder an, die dynamisch hinzugefügt werden.

So erstellen Sie eine statische Gruppe:

1. Wählen Sie in der -Benutzerkonsole die Optionen "Gruppen", "Gruppe erstellen" aus.
2. Entscheiden Sie, ob Sie eine neue Gruppe oder eine Kopie einer Gruppe erstellen möchten, und klicken Sie auf **OK**.
3. Geben Sie auf der Registerkarte "Profil" einen Gruppennamen, eine Gruppenorganisation, eine Beschreibung und einen Gruppenadministratornamen ein.
4. Klicken Sie auf die Registerkarte "Mitgliedschaft".
5. Klicken Sie auf "Benutzer hinzufügen".
6. Suchen Sie Benutzer, die aufgenommen werden sollen.
7. Aktivieren Sie das Häkchen neben den Benutzern, und klicken Sie auf "Auswählen".
8. Klicken Sie auf "Submit".

Erstellen einer dynamischen Gruppe

Um eine *dynamische Gruppe* zu erstellen, definieren Sie über die Benutzerkonsole eine LDAP-Filterabfrage, damit die Gruppenmitgliedschaft dynamisch zur Laufzeit ermittelt wird, ohne dass Sie nach einzelnen Benutzern suchen und diese hinzufügen müssen.

Wenn Sie z. B. eine Gruppe erstellen möchten, die alle US-Arbeitnehmer von NeteAuto auflistet, können Sie einen LDAP-Suchfilter im Feld "Dynamische Gruppenabfrage" der Benutzerkonsole erstellen, der wie folgt aussieht:

ldap:///cn=Arbeitnehmer,o=NeteAuto,c=US??sub

Sie können diese Abfrage auch ändern, um nach Arbeitnehmern außerhalb der USA zu suchen.

Beispiel für statische, dynamische und verschachtelte Gruppen (siehe Seite 175): In diesem Beispiel ist eine Gruppe dargestellt, die von statischen, dynamischen und verschachtelten Gruppen erstellt wurde.

Hinweis: Das Feld "Dynamische Gruppenabfrage" schließen Sie in der Aufgabe ein, indem Sie das verknüpfte Profilfenster bearbeiten. Das Feld ist in der Aufgabe "Gruppe erstellen" standardmäßig nicht enthalten.

So erstellen Sie eine dynamische Gruppe:

1. Wählen Sie in der Benutzerkonsole die Optionen "Gruppen", "Gruppe erstellen" aus.
2. Entscheiden Sie, ob Sie eine neue Gruppe oder eine Kopie einer Gruppe erstellen möchten, und klicken Sie auf **OK**.
3. Geben Sie auf der Registerkarte "Profil" einen Gruppennamen, eine Gruppenorganisation, eine Beschreibung und einen Gruppenadministratornamen ein.
4. Geben Sie im Feld "Dynamische Gruppenabfrage" einen LDAP-Suchfilter gemäß dem folgenden Beispiel ein:

   ldap:///cn=Arbeitnehmer,o=NeteAuto,c=US??sub?
5. Klicken Sie auf "Senden".

Hinweis: Nur Administratoren, die über die Aufgabe "Gruppe ändern" verfügen, können die dynamische Mitgliedschaft einer Gruppe ändern.

Parameter für dynamische Gruppenabfragen

In der Suche können Sie die folgenden Parameter für dynamische Abfragen verwenden:

ldap:///*<Such-Basis-DN>*??*<Suchbereich>*?*<Suchfilter>*

- *<Such-Basis-DN>*: Hierbei handelt es sich um den Ausgangspunkt für Suchen im LDAP-Verzeichnis. Falls Sie die Basis-DN in der Abfrage nicht angeben, wird die Organisation der Gruppe als Such-Basis-DN verwendet.
- *<Suchbereich>*: Hiermit wird das Ausmaß der Suche angegeben. Hierzu zählt:
  - sub: Gibt Einträge auf Basis-DN-Ebene und darunter zurück
  - one: Gibt Einträge eine Ebene unterhalb der Basis-DN zurück, die Sie im URL angeben (Standard)
  - base: Verwendet alternativ "one", die Basis wird als Suchoption ignoriert

  Bei Verwendung von one oder base werden nur die Benutzer in der Basis-DN-Organisation abgerufen.

  Bei Verwendung von sub werden alle Benutzer unter der Basis-DN-Organisation und allen Unterorganisationen in der Struktur abgerufen.

- *<Suchfilter>*: Hierbei handelt es sich um den Filter, den Sie auf die Einträge im Suchbereich anwenden möchten. Verwenden Sie beim Eingeben eines Suchfilters die standardmäßige LDAP-Abfragesyntax gemäß folgendem Beispiel:

  (<logischer Operator><Vergleich><Vergleich...>)

  - Bei <logischer Operator> kann es sich um einen der folgenden Werte handeln:

    Logisches OR: |

    Logisches AND: &

    Logisches NOT: !

  - <Vergleich> gibt <Attribut><Operator><Wert> an

  Beispiel:

  (&(city=boston)(state=Massachusetts))

  Beim Standardsuchfilter handelt es sich um (objectclass=*).

Beachten Sie beim Erstellen einer dynamischen Abfrage Folgendes:

- Das "ldap"-Präfix muss klein geschrieben sein, zum Beispiel:

  ldap:///o=MyCorporation??sub?(title=Manager)

- Sie können den Hostnamen und die Portnummer des LDAP-Servers nicht angeben. Alle Suchen treten innerhalb des LDAP-Verzeichnisses auf, das der Umgebung zugeordnet ist.

Die folgende Tabelle enthält Beispiel-LDAP-Abfragen:

Beschreibung	**Abfrage**
Alle Benutzer, bei denen es sich um Manager handelt.	ldap:///o=MyCorporation??sub?(title=Manager)
Alle Manager der Zweigstelle "New York West"	ldap:///o=MeinUnternehmen??one?(&(title=Manager) (roomNumber=NYWest))
Alle Techniker mit Mobiltelefonen	ldap:///o=MeinUnternehmen??one? (&(employeetype=Techniker) (mobile=*))
Alle Arbeitnehmer, deren Arbeitnehmernummer zwischen 1000 und 2000 liegt	ldap:///o=MeinUnternehmen, (& (ou=Arbeitnehmer) (employeenumber >=1000) (employeenumber <=2000))
Alle Helpdesk-Administratoren, die seit über sechs Monaten beim Unternehmen beschäftigt sind	ldap:///o=MeinUnternehmen,(& (cn=Helpdesk-Administrator) (DOH => 2004/04/22) **Hinweis:** Für diese Abfrage ist es erforderlich, dass Sie für das Einstelldatum (date of hire, DOH) des Benutzers ein DOH-Attribut erstellen.

Hinweis: Die Vergleichssymbole ">" und "<" (größer und kleiner als) werden im lexikografischen, nicht im arithmetischen Sinne verwendet. Hinweise zu deren Verwendung finden Sie in der Dokumentation zu Ihrem LDAP-Verzeichnisserver.

Erstellen von verschachtelten Gruppen

Wenn es sich beim Benutzerspeicher um ein LDAP-Verzeichnis handelt, können Sie eine Gruppe als Mitglied einer anderen Gruppe hinzufügen. Diese Gruppe wird als *verschachtelte Gruppe* bezeichnet.

Die Gruppe, die die verschachtelte Gruppe enthält, bezeichnet man als *übergeordnete Gruppe*. Mitglieder der verschachtelten Gruppe werden zu Mitgliedern der übergeordneten Gruppe. Die Mitglieder der übergeordneten Gruppe werden jedoch keine Mitglieder der verschachtelten Gruppe.

Verschachtelte Gruppen ähneln Verteilerlisten für E-Mails, bei denen eine Liste Mitglied einer anderen Liste sein kann. Bei verschachtelten Gruppen können Sie Gruppen und Benutzer als Mitglieder zur Gruppe hinzufügen. Durch Verschachteln einer Gruppe in der Mitgliederliste einer anderen Gruppe können Sie alle Mitglieder der verschachtelten Gruppe einschließen.

Wenn Sie beispielsweise separate Gruppen für die Fertigungs-, Entwurfs-, Versand- und Buchhaltungsabteilungen eines Unternehmens erstellt haben, können Sie eine übergeordnete Gruppe für das gesamte Unternehmen erstellen, indem Sie alle separaten Abteilungsgruppen als Mitglieder in der übergeordneten Unternehmensgruppe verschachteln. Daher werden alle Änderungen, die Sie an den verschachtelten Fertigungs-, Entwurfs-, Versand- und Buchhaltungsgruppen vornehmen, automatisch auch in der verschachtelten Gruppe für das gesamte Unternehmen vorgenommen. Bei in anderen Gruppen verschachtelten Gruppen kann es sich um dynamische Gruppen handeln, die auch andere verschachtelte Gruppen enthalten können.

Die Abbildung unter Beispiel für statische, dynamische und verschachtelte Gruppen (siehe Seite 175) stellt eine übergeordnete Gruppe dar, die von statischen, dynamischen und verschachtelten Gruppen erstellt wurde.

Beachten Sie vor dem Erstellen verschachtelter Gruppen folgende Punkte:

- Nur Administratoren mit der Aufgabe "Gruppenmitglieder ändern" können verschachtelte Gruppen von der statischen Mitgliederliste der Gruppe in der -Benutzerkonsole hinzufügen oder ändern.
- Nur Benutzer mit den entsprechenden Administratorberechtigungen können Mitglieder einer Gruppe ändern, zu dieser hinzufügen oder aus dieser entfernen.

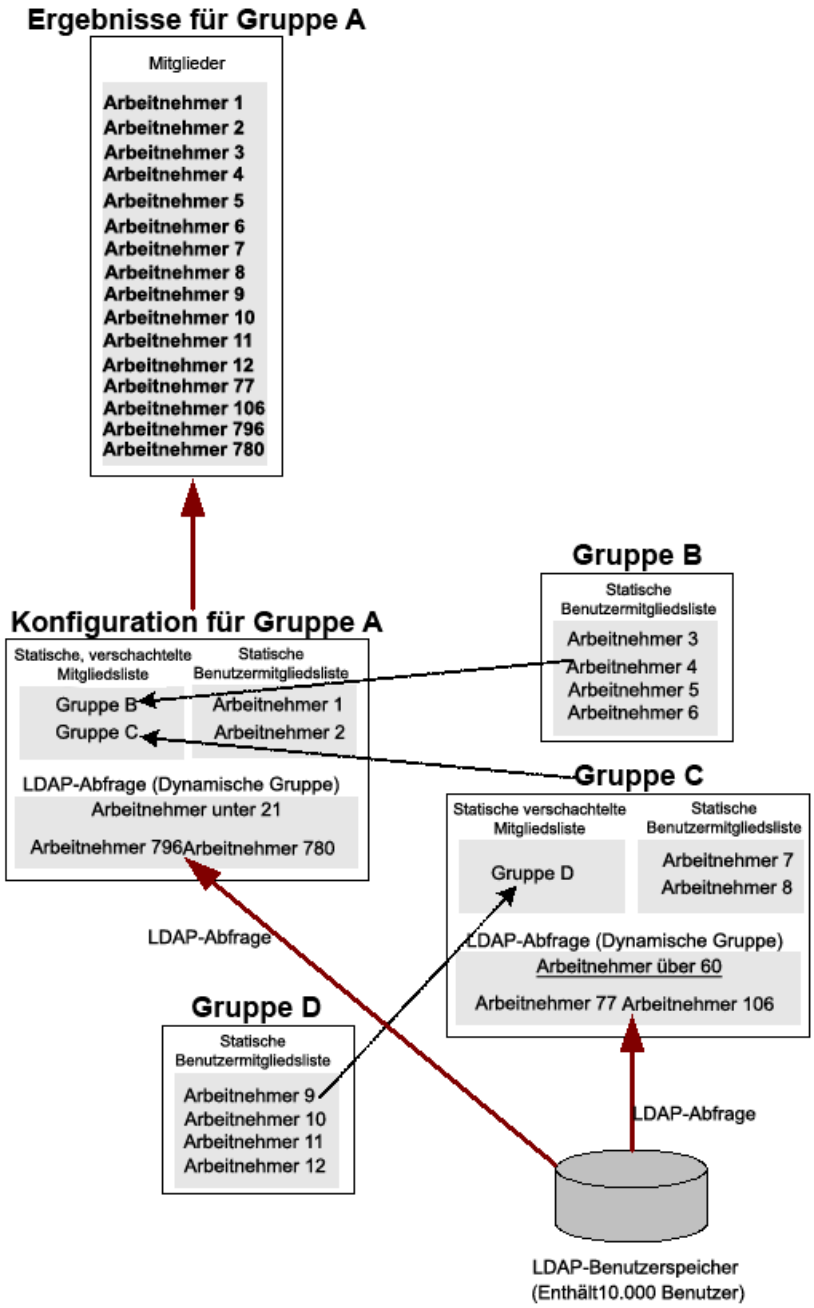
  Falls eine übergeordnete Gruppe A beispielsweise durch die verschachtelten Gruppen B und C erstellt wird, kann der Administrator von Gruppe A nur die Mitglieder von Gruppe A, nicht jedoch von B und C ändern. Die Gruppen B und C können nur von ihren jeweiligen Administratoren geändert werden.

So erstellen Sie eine verschachtelte Gruppe:

1. Wählen Sie in der -Benutzerkonsole die Optionen "Gruppen", "Gruppe erstellen" aus.
2. Entscheiden Sie, ob Sie eine neue Gruppe oder eine Kopie einer Gruppe erstellen möchten, und klicken Sie auf **OK**.
3. Geben Sie auf der Registerkarte "Profil" einen Gruppennamen, eine Gruppenorganisation, eine Beschreibung und einen Gruppenadministratornamen ein.
4. Auf der Registerkarte "Mitgliedschaft":
   a. Klicken Sie auf die Option "Eine Gruppe hinzufügen", um dieser Gruppe eine verschachtelte Gruppe hinzuzufügen.
   b. Suchen Sie nach einer vorhandenen Gruppe.
   c. Wählen Sie die Gruppe mit einem Häkchen aus, und klicken Sie auf die Option "Auswählen".
   d. Klicken Sie auf "Submit".

Beispiel für statische, dynamische und verschachtelte Gruppen

Gruppen können komplex sein und aus einer Kombination von dynamischen, statischen und verschachtelten Gruppen bestehen. In der folgenden Abbildung ist ein Beispiel für eine übergeordnete Gruppe dargestellt, die durch statische, dynamische und verschachtelte Gruppen erstellt wurde.



Zur vorstehenden Abbildung:

- Die übergeordnete Gruppe A enthält die verschachtelten Gruppen B und C, zwei statische Benutzer und eine dynamische LDAP-Abfrage, die alle Arbeitnehmer unter 21 Jahren aufführt.
- Gruppe B besteht aus vier statischen Benutzern.
- Die übergeordnete Gruppe C enthält die verschachtelte Gruppe D, zwei statische Benutzer und eine dynamische LDAP-Abfrage, die alle Arbeitnehmer über 60 Jahre aufführt.
- Gruppe D enthält vier statische Benutzer.
- Oben in der Abbildung sind die Mitglieder der Gruppe A aufgeführt, die aus den verschachtelten Gruppen, den dynamischen Abfragen und den statischen Benutzermitgliedslisten der Gruppen B, C und D resultieren.

Gruppenadministratoren

In der Aufgabe "Gruppe erstellen" bzw. "Gruppe ändern" können Sie auf der Registerkarte "Administratoren" Benutzer und Gruppen als Administratoren einer Gruppe angeben. Stellen Sie beim Zuweisen eines Benutzers zu einer Gruppe als Administrator sicher, dass der Administrator eine Rolle mit entsprechendem Bereich zum Verwalten der Gruppe aufweist. Beispiel:

1. Verwenden Sie die Option "Gruppe ändern", um einen Benutzer einer Gruppe als Administrator zuzuweisen.
2. Weisen Sie diesem Benutzer eine Admin-Rolle mit Gruppenverwaltungsaufgaben (z. B. "Gruppenmitglieder ändern") bzw. Benutzerverwaltungsaufgaben zu, die eine Registerkarte "Gruppen" aufweisen.
3. Prüfen Sie, ob die Rolle den entsprechenden Bereich über die Gruppe aufweist.
    a. Verwenden Sie bei der Rolle, die Sie mit Gruppenverwaltungsaufgaben zugewiesen haben, die Option "Admin-Rolle anzeigen".
    b. Stellen Sie sicher, dass auf der Registerkarte "Mitglieder" eine Richtlinie vorhanden ist, die folgenden Kriterien erfüllt:

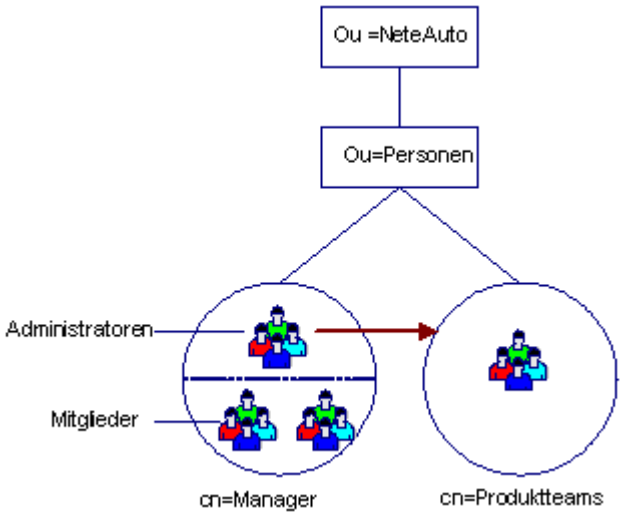
        Eine Mitgliederregel, die der Gruppenadministrator erfüllt

        Eine Bereichsregel, die die Gruppe enthält

        Eine Bereichsregel, die Benutzer enthält, welche zur Gruppe hinzugefügt werden sollen

Hinweis: Um in einer IdentityMinder-Umgebung Gruppen als Administratoren anderer Gruppen zu aktivieren, konfigurieren Sie in der Verzeichniskonfigurationsdatei die Gruppenadministratorunterstützung. Weitere Informationen finden Sie im *Konfigurationshandbuch*.

Beim Zuweisen von Gruppen als Administratoren werden nur Administratoren dieser Gruppe zu Administratoren der Gruppe, die Sie erstellen oder ändern. Mitglieder der Administratorgruppe, die Sie angeben, weisen keine Berechtigungen zum Verwalten der Gruppe auf. In der folgenden Abbildung ist eine Gruppe als Administrator einer anderen Gruppe dargestellt.



In diesem Beispiel gilt Folgendes:

- Die Gruppe "Manager" ist ein Administrator der Gruppe "Produktteams".
- Administratoren der Gruppe "Manager" können die Gruppe "Produktteams" verwalten. Mitglieder der Gruppe "Manager" weisen diese Berechtigung nicht auf.

Kapitel 8: Konten an verwalteten Endpunkten

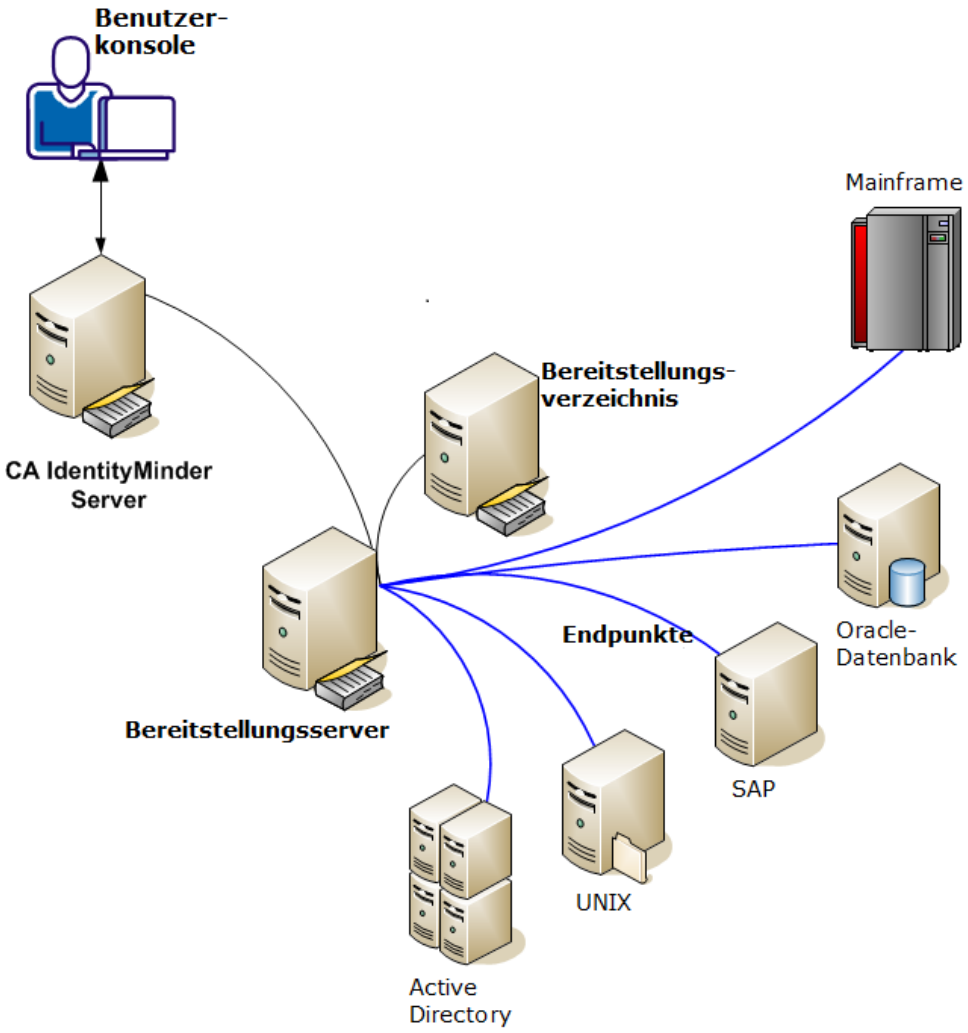
Sie können in CA IdentityMinder Konten auf Endpunktsystemen verwalten, sofern Ihre CA IdentityMinder-Installation über einen Bereitstellungsserver verfügt. Dazu gehören z. B. Exchange-, Windows NT- und Oracle-Konten sowie verwaiste Konten und Systemkonten, also Konten, die derzeit nicht mit CA IdentityMinder in Verbindung stehen.

Dieses Kapitel enthält folgende Themen:

Integrieren von verwalteten Endpunkten (siehe Seite 180)
Benutzer, Konten, und Rollen synchronisieren (siehe Seite 187)
Umgekehrte Synchronisierung mit Endpunktkonten (siehe Seite 195)
Erweitern der benutzerdefinierten Attribute an Endpunkten (siehe Seite 207)
Kontoaufgaben (siehe Seite 209)
Erweiterte Kontovorgänge (siehe Seite 215)

Integrieren von verwalteten Endpunkten

Mit CA IdentityMinder können Sie Konten auf mehreren Systemen von einer einzelnen Benutzeroberfläche verwalten, der Benutzerkonsole. Die Konten befinden sich auf Systemen, die als verwaltete Endpunkte oder einfach Endpunkte bezeichnet werden. Im folgenden Beispiel verwalten Sie Benutzer auf fünf Endpunkten.



Sie können einem Benutzer Konten auf einer beliebigen Kombination von Endpunkten zuweisen. Wenn Sie einen Endpunkt integrieren, ordnet CA IdentityMinder jedem Endpunkt-Benutzerkonto einen Benutzer im Bereitstellungsverzeichnis zu.

Die folgenden Vorgänge beschreiben, wie Sie Endpunkte integrieren, sodass Endpunkt-Benutzerkonten von der Benutzerkonsole verwaltet werden können.

1. Importieren der Rollendefinitions-Datei (siehe Seite 181)
2. Erstellen von Korrelationsregeln (siehe Seite 181)
3. Hinzufügen des Endpunkts zu der Umgebung (siehe Seite 184)
4. Erstellen einer Definition "Durchsuchen und Korrelieren" (siehe Seite 184)
5. Durchsuchen und Korrelieren des Endpunkts (siehe Seite 186)

Importieren der Rollendefinitions-Datei

Sie importieren die Rollendefinitionen aus einer Datei, die sich auf den neuen Endpunkt bezieht. Dieser Vorgang benötigt Zugriff auf die Management-Konsole.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Management-Konsole auf "Umgebungen".
2. Wählen Sie die Umgebung aus, in der Sie den Endpunkt hinzufügen.
3. Klicken Sie auf "Rollen- und Aufgabeneinstellungen".
4. Klicken Sie auf "Importieren".
5. Wählen Sie unter "Endpunkttyp" einen Endpunkt aus.
6. Klicken Sie auf "Fertig stellen".

   Der Status des Imports wird im aktuellen Fenster angezeigt.
7. Klicken Sie zum Beenden auf "Fortfahren".
8. Starten Sie die Umgebung neu, sodass die Änderungen in Kraft treten.

Erstellen von Korrelationsregeln

Ein Hosting-Administrator oder ein Administrator mit der Aufgabe "Korrelationsattribute konfigurieren" kann Regeln erstellen, die verwendet werden, wenn Sie einen Endpunkt durchsuchen. Die Aufgabe "'Durchsuchen und Korrelieren' ausführen" verwendet diese Regeln für den Korrelationsteil der Aufgabe.

Korrelationsregeln entscheiden, wie ein Endpunkt-Benutzerkonto-Attribut einem Benutzerattribut in der Benutzerkonsole zugeordnet wird. Zum Beispiel ist in Access Control ein Attribut "AccountName" vorhanden. Sie können eine Regel erstellen, um es "FullName" in der Benutzerkonsole zuzuordnen. Wenn die Regeln dazu führen, dass zwei Zuordnungen für ein Benutzerattribut gelten, wird der erste Parameterwert verwendet.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole an.
2. Klicken Sie auf "System", "Bereitstellungskonfiguration", "Korrelationsattribute konfigurieren".
3. Klicken Sie auf Hinzufügen.
4. Definieren Sie eine Korrelationsregel wie folgt:
   a. Wählen Sie eine globale Benutzerattributliste aus.

      Dieser Wert bezieht sich auf das im Bereitstellungsverzeichnis aufgelistete Benutzerattribut.

   b. Aktivieren Sie das Kontrollkästchen "Ein bestimmtes Kontenattribut festlegen".
   c. Wählen Sie einen Endpunktyp aus.
   d. Wählen Sie ein Kontoattribut aus, das sich auf das globale Benutzerattribut bezieht.
   e. Füllen Sie optional die Unterzeichenfolgen-Felder aus.

      Wenn das Feld "Unterzeichenfolge von" leer ist, fängt die Verarbeitung am Anfang der Zeichenfolge an. Wenn das Feld "Unterzeichenfolge von" leer ist, fängt die Verarbeitung am Anfang der Zeichenfolge an.
5. Klicken Sie auf "OK".
6. Klicken Sie auf "Senden".

Hinweis: Immer wenn Sie eine Korrelationsregel ändern, müssen Sie den Endpunkt durchsuchen, auch wenn Sie ihn zuvor durchsucht haben.

Beispiel für Korrelationsregeln

Das folgende Beispiel enthält Beispieleinstellungen für einen Active Directory-Endpunkt.

```
GlobalUserName
FullName=LDAP Namespace:globalFullName
FullName=ActiveDirectory:DisplayName
 CustomField01=ActiveDirectory:Telephone
```

Die folgenden Aktionen treten für jedes zuvor unkorrelierte Konto auf, das gefunden wird, während Konten in einem Active Directory-Container korreliert werden:

1. Der Bereitstellungsserver vergleicht den ersten Parameterwert (GlobalUserName) mit dem Active Directory-Endpunkt-Benutzerkonto-Attribut (NT_AccountID). Der Server versucht, den eindeutigen globalen Benutzer zu finden, dessen Name mit dem NT_AccountID-Attributwert für dieses Konto übereinstimmt. Wenn eine eindeutige Übereinstimmung gefunden wird, ordnet der Bereitstellungsserver das Konto dem globalen Benutzer zu. Wenn mehr als eine Übereinstimmung gefunden wird, führt der Bereitstellungsserver Schritt 5 aus. Wenn keine Übereinstimmung gefunden wird, führt der Bereitstellungsserver den nächsten Schritt aus.
2. Der Bereitstellungsserver beachtet den zweiten Parameterwert (FullName=LDAP Namespace:globalFullName). Da dieser Wert spezifisch für einen anderen Endpunkttyp ist, wird er übersprungen, und der Bereitstellungsserver führt den nächsten Schritt aus.
3. Der Bereitstellungsserver beachtet den dritten Parameterwert (FullName=ActiveDirectory:DisplayName). Da dieser Wert spezifisch für Active Directory ist, wird er verwendet. Der Server versucht, den eindeutigen globalen Benutzer zu finden, dessen Name mit dem Anzeigenamen-Attributwert für dieses Konto übereinstimmt. Wenn eine eindeutige Übereinstimmung gefunden wird, ordnet der Bereitstellungsserver das Konto dem globalen Benutzer zu. Wenn mehr als eine Übereinstimmung gefunden wird, führt der Bereitstellungsserver Schritt 5 aus. Wenn keine Übereinstimmung gefunden wird, führt der Bereitstellungsserver Schritt 4 aus.
4. Der Bereitstellungsserver beachtet den letzten Parameterwert (CustomField01=ActiveDirectory:Telephone). Da dieser Wert spezifisch für Active Directory ist, wird er verwendet. Der Server versucht, den eindeutigen globalen Benutzer zu finden, dessen "Custom Field #01"-Attribut gleich dem "Telephone"-Attributwert für dieses Konto ist. Der Name, den Sie dem benutzerdefinierten globalen Benutzerattribut mithilfe globaler Eigenschaften der Systemaufgabe zugewiesen haben, wird hier nicht angezeigt. Wenn eine eindeutige Übereinstimmung gefunden wird, ordnet der Bereitstellungsserver das Konto dem globalen Benutzer zu. Wenn mehr als eine Übereinstimmung gefunden wird, führt der Bereitstellungsserver Schritt 5 aus. Wenn keine Übereinstimmung gefunden wird, führt der Bereitstellungsserver den nächsten Schritt aus.
5. Der Bereitstellungsserver ordnet das Konto dem Objekt [Standardbenutzer] zu. Wenn das Objekt [Standardbenutzer] nicht vorhanden ist, wird es vom Server erstellt.

Hinzufügen des Endpunkts zu der Umgebung

Sie fügen den Endpunkt der Umgebung hinzu, in der Sie es verwalten möchten. Jeder Administrator mit der Aufgabe "Endpunkt erstellen" kann diesen Vorgang ausführen.

Gehen Sie wie folgt vor:

1. Wählen Sie "Endpunkt auswählen", "Endpunkte verwalten", "Endpunkt erstellen".
2. Wählen Sie einen Endpunktyp aus.
3. Füllen Sie die Felder auf den Registerkarten aus.

   Die Pflichtfelder beginnen mit einem roten Kreis. Klicken Sie auf "Hilfe", um Informationen zu den Felddefinitionen auf der aktuellen Registerkarte zu erhalten.

   Hinweis: Verwenden Sie kein "#" im Endpunktnamen, da nach diesem Zeichen nicht gesucht werden kann.
4. Klicken Sie auf "Senden".

Nun können Sie eine Definition "Durchsuchen und Korrelieren" (siehe Seite 184) erstellen, damit dessen Konten verwaltet werden können.

Erstellen einer Definition "Durchsuchen und Korrelieren"

Um Benutzer hinzuzufügen, die in einem Endpunkt vorhanden sind, erstellen Sie eine Definition "Durchsuchen und Korrelieren" für diesen Endpunkt. Jeder Administrator mit der Aufgabe "Definition 'Durchsuchen und Korrelieren' erstellen" kann die Definition erstellen.

Gehen Sie wie folgt vor:

1. Klicken Sie in einer Umgebung auf "Endpunkte", "Definitionen 'Durchsuchen und Korrelieren'", "Definition 'Durchsuchen und Korrelieren' erstellen".
2. Klicken Sie auf "OK", um eine neue Definition zu erstellen.
3. Geben Sie in "Name von Durchsuchen und Korrelieren" eine aussagekräftige Bezeichnung ein.
4. Klicken Sie auf "Container/Endpunkt/Durchsuchungsmethode auswählen", um einen Endpunkt und Container zu wählen, wenn sie vorhanden sind. Für einen großen Endpunkt kann eine Containersuche eine Weile dauern. Sie können den Suchfilter verwenden, um die Suche einzuschränken.
5. Klicken Sie auf eine Durchsuchungsmethode für den Container. Der Vorgang für das Durchsuchen und Korrelieren bezieht die von Ihnen ausgewählten Container und deren Untercontainer mit ein. Bei einem Verzeichniscontainer werden alle Container in der Unterstruktur berücksichtigt.

6. Klicken Sie unter "Aktion Durchsuchen/Korrelieren" auf die Aktion, die durchgeführt werden soll:
   - **Verzeichnis nach verwalteten Objekten durchsuchen** - Sucht nach Objekten, die am Endpunkt und nicht im Bereitstellungsverzeichnis gespeichert sind.
   - **Konten an Benutzer korrelieren** - Korreliert die von der Suchfunktion gefundenen Objekte mit Benutzern im Bereitstellungsverzeichnis. Es gibt zwei Korrelationsoptionen.
     - **Vorhandenen Benutzer verwenden**

       Verwenden Sie diese Option für eine Korrelationsregel (siehe Seite 181), die jedes Konto mit einem zuvor erstellten Benutzer abgleicht.

       Wird der Benutzer gefunden, wird das Objekt mit dem Benutzer korreliert. Wenn mehrere Benutzer gefunden werden, wird der Benutzer mit dem Standardbenutzer korreliert. Wenn kein Benutzer gefunden wird, erstellt diese Option den Benutzer (wenn alle obligatorischen Attribute bekannt sind) und korreliert das Konto mit diesem Benutzer; sonst wird das Konto mit dem Standardbenutzer korreliert.
     - **Benutzer nach Bedarf erstellen**

       Verwenden Sie diese Option, wenn Sie Konten auf dem primären Endpunkt korrelieren. Bei dieser Option wird vorausgesetzt, dass die Konten am Endpunkt exakt dieselben Namen wie die Benutzer haben. Der Korrelations-Übereinstimmungs-Algorithmus wird mit dieser Option nicht verwendet. Jedes Konto wird einfach dem Benutzer mit demselben Namen zugeordnet. Wenn der Benutzer noch nicht vorhanden ist, wird er erstellt. Mit dem Standardbenutzer werden keine Konten verbunden.
   - **Benutzerfelder aktualisieren** - Falls zwischen den Objektfeldern und den Benutzerfeldern eine Zuordnung besteht, werden die Benutzerfelder mit den Daten der Objektfelder aktualisiert.

     Benutzer werden mit keinen optionalen Attributen wie vollständiger Name, Adresse und Telefonnummern erstellt. Verwenden Sie diese Option während des ursprünglichen Abrufs eines Endpunkts zum Festlegen dieser Attribute für Benutzer durch Werte von Kontoattributen. Während nachfolgender Durchsuchungs- und Korrelierungsvorgänge verwenden Sie diese Option, um die Benutzerattribute zu aktualisieren und vorgenommene Änderungen auf die Kontoattribute anzuwenden, ggf. von anderen Tools als CA IdentityMinder.
7. Klicken Sie auf "Senden".

Nun führt ein Administrator mit der Aufgabe "Durchsuchen und Korrelieren" ausführen (siehe Seite 186) die Integration des Endpunkts aus.

Durchsuchen und Korrelieren des Endpunkts

Ein Hosting-Administrator oder ein anderer Administrator mit der Aufgabe "'Durchsuchen und Korrelieren' ausführen" führt diesen Vorgang aus. In der Durchsuchungsphase der Aufgabe werden die Konten im Endpunkt identifiziert. In der Korrelationsphase werden die Konten mit Benutzern in CA IdentityMinder abgeglichen oder die Konten erstellt.

Gehen Sie wie folgt vor:

1. Klicken Sie in einer Umgebung auf "Endpunkte", "'Durchsuchen und Korrelieren' ausführen".
2. Wählen Sie "Jetzt ausführen" aus, um Durchsuchen und Korrelieren sofort auszuführen, oder wählen Sie Neuen Job planen (siehe Seite 443) aus, um Durchsuchen und Korrelieren zu einem späteren Zeitpunkt oder nach einem Zeitplan auszuführen.

   Hinweis: Für diesen Vorgang muss sich der Client-Browser in derselben Zeitzone wie der Server befinden. Wenn beispielsweise die Uhrzeit auf dem Client 22:00 Uhr und die Serverzeit 7:00 Uhr beträgt, funktioniert die "Definition "Durchsuchen und Korrelieren" nicht.
3. Klicken Sie auf die Definition für das Durchsuchen und Korrelieren, die ausgeführt werden soll.
4. Klicken Sie auf "Senden".

   Die am Endpunkt vorhandenen Benutzerkonten werden in CA IdentityMinder basierend auf der von Ihnen erstellten Definition "Durchsuchen und Korrelieren" erstellt oder aktualisiert.
5. Überprüfen Sie folgendermaßen den Erfolg der Aufgabe:
   a. Klicken Sie auf "System", "Gesendete Aufgaben anzeigen".
   b. Geben Sie Folgendes in das Feld "Aufgabenname" ein: "Durchsuchen und Korrelieren ausführen".
   c. Klicken Sie auf Suchen.

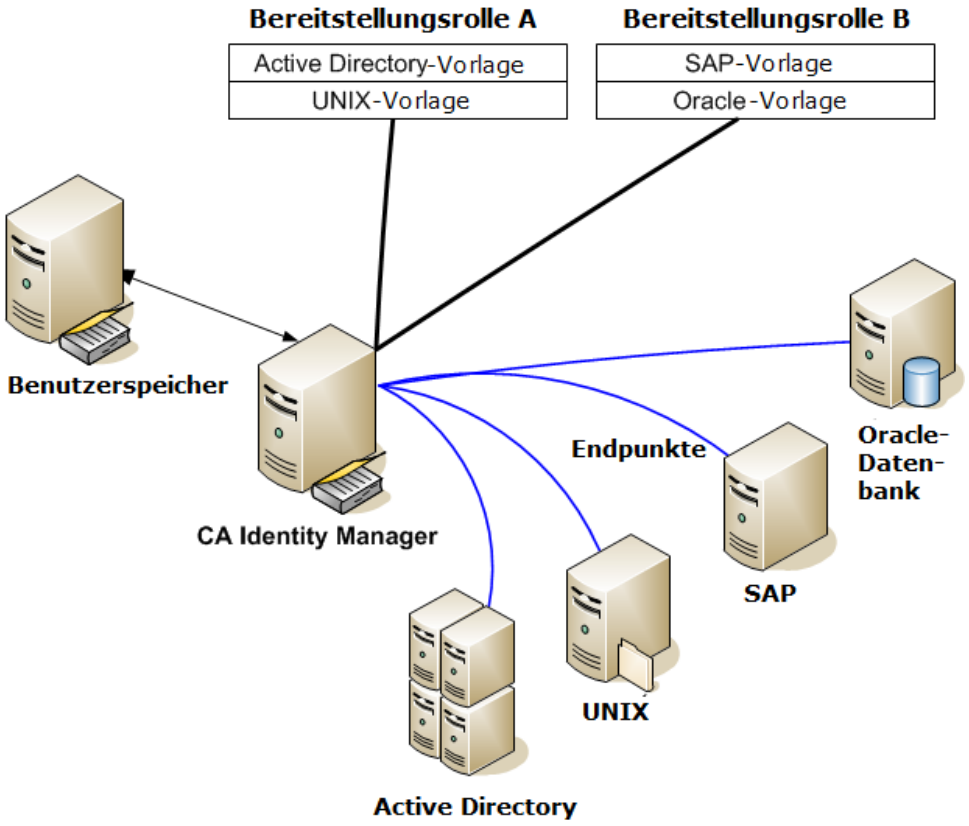
   Die Ergebnisse zeigen, ob die Aufgabe erfolgreich abgeschlossen wurde.

Hinweis: Sie können eine Aufgabe "Durchsuchen und Korrelieren" abbrechen, wenn Sie den Aufgabenstatus in "Gesendete Aufgaben anzeigen" (VST). Das Abbrechen der Aufgabe hält die Aufgabe von der Ausführung ab, und hinterlässt sie in dem Status, in dem sie sich befindet, wenn Sie sie abbrechen. Sämtliche generierte Benachrichtigungen werden gesendet, sodass alle Systeme synchronisiert gehalten werden.

Benutzer, Konten, und Rollen synchronisieren

Die Integration mehrerer Endpunkte und Konten in ein einzelnes Benutzerverwaltungssystem kann darin resultieren, dass keine Synchronisierung erfolgt. Die Bereitstellungsrollen oder Kontovorlagen, die einem Benutzer zugewiesen werden, können sich von den eigentlichen Konten für diesen Benutzer unterscheiden.

Stellen Sie sich beispielsweise ein Szenario mit zwei Bereitstellungsrollen vor, eine mit Active Directory- und UNIX-Kontovorlagen und eine andere mit SAP- und Oracle-Vorlagen. Der Benutzer john_smith hat die Bereitstellungsrolle A, die Active Directory- und UNIX-Kontovorlagen umfasst, aber nur ein Active Directory-Konto. Möglicherweise wurde die UNIX-Kontovorlage der Rolle hinzugefügt, nachdem sie dem Benutzer zugewiesen wurde. Daher synchronisiert der Administrator den Benutzer mit der aktuellen Rollendefinition.



In den folgenden Fällen findet ebenfalls keine Synchronisierung mit Bereitstellungsrollen oder Kontovorlagen für Benutzer statt:

- Frühere Versuche, die notwendigen Konten zu erstellen, schlugen aufgrund von Hardware- oder Softwareproblemen in Ihrem Netzwerk fehl, was zu fehlenden Konten führte.
- Bereitstellungsrollen und Kontovorlagen ändern sich. Dadurch entstehen zusätzliche oder fehlende Konten.
- Konten wurden Kontovorlagen nach ihrer Erstellung zugewiesen. Das heißt, es sind Konten vorhanden, aber sie werden nicht mit ihren Kontovorlagen synchronisiert.
- Die Erstellung eines neuen Kontos wird verschoben, da die Kontoerstellung auf einen späteren Zeitpunkt festgelegt wurde.
- Ein neuer Endpunkt wurde erworben. Während dem Durchsuchen und Korrelieren hat der Bereitstellungsserver den Benutzern nicht automatisch Bereitstellungsrollen zugewiesen. Sie aktualisieren die Rolle, um die Benutzer anzuzeigen, die Endpunktkonten benötigen. Ein Konto, das zu einem Benutzer korreliert wurde, wird bei der Synchronisierung des Benutzers als zusätzliches Konto aufgelistet.
- Ein vorhandenes Konto wurde einem Benutzer durch Kopieren des Kontos zugewiesen.
- Ein Konto wurde nicht durch Zuweisen des Benutzers zu einer Rolle für einen Benutzer erstellt. Zum Beispiel haben Sie einen Benutzer in eine Kontovorlage kopiert, die sich in keiner Bereitstellungsrolle für diesen Benutzer befindet. Das Konto wird als zusätzliches Konto oder als Konto mit einer zusätzlichen Kontovorlage aufgelistet. Wenn Sie den Benutzer zu einem Endpunkt kopieren, um mit der Standardkontovorlage ein Konto zu erstellen, könnte es sich bei diesem Konto um ein zusätzliches Konto handeln.

Die folgenden Abschnitte erklären, wie sie die drei Typen der Synchronisierung ausführen:

1. Benutzer mit Rollen synchronisieren (siehe Seite 189)
2. Benutzer mit Kontovorlagen synchronisieren (siehe Seite 191)
3. Endpunktkonto mit Kontovorlagen synchronisieren (siehe Seite 190)

Benutzer mit Rollen synchronisieren

Diese Aufgabe erstellt, aktualisiert, oder löscht Konten, sodass sie den Bereitstellungsrollen entsprechen, die einem Benutzer zugewiesen wurden. Zum Beispiel verwenden Administratoren systemeigene Tools auf einem Endpunkt, um Konten hinzuzufügen oder zu löschen, aber Sie haben diesen Endpunkt nicht erneut durchsucht, um das Bereitstellungsverzeichnis zu aktualisieren. Deswegen haben Benutzer zusätzliche oder fehlende Konten. Diese Aufgabe stellt auch sicher, dass jedes Konto zu den richtigen Kontovorlagen gehört.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole an.
2. Wählen Sie "Benutzer", "Synchronisierung", "Synchronisierung der Rolle überprüfen".
3. Wählen Sie einen Benutzer aus.

   Ein Fenster mit den erwarteten, zusätzlichen und fehlenden Konten wird angezeigt.
4. Klicken Sie auf "Synchronisieren", um die Konten mit der Vorlage in dieser Rolle zu synchronisieren.
   a. Sie können ein Kontrollkästchen aktivieren, um das Konto auf dem Endpunkt zu erstellen. Wenn mehr als eine Kontovorlage für den Benutzer das gleiche Konto vorschreibt, wird das Konto durch das Zusammenführen aller relevanten Kontovorlagen erstellt.

      Dieses Konto wird den Kontovorlagen zugewiesen, die gegenwärtig nicht mit dem Konto synchronisiert sind.

   b. Sie können ein Kontrollkästchen aktivieren, um zusätzliche Konten zu löschen. Allerdings können Benutzer berechtigte Gründe für den Besitz dieser Konten haben. Lassen Sie diese Option dann deaktiviert.

      Auf gewissen Endpunkten ist die Kontolöschungsfunktion deaktiviert; daher wird das Konto nicht gelöscht.

Benutzer mit Kontovorlagen synchronisieren

Diese Aufgabe synchronisiert die Attribute für Endpunktkonten mit den zugeordneten Kontovorlagen für einen Benutzer. Allerdings hängt die volle Synchronisierung von folgenden Faktoren ab:

- Die volle Synchronisierung des Kontos erfolgt in zwei Fällen. Eine Kontovorlage nutzt die starke Synchronisierung, (siehe Seite 192) oder zwei oder mehr Kontovorlagen wurden einem Konto hinzugefügt.
- Wenn eine Kontovorlage die schwache Synchronisierung (siehe Seite 192) nutzt, startet diese Aufgabe nur für diese Vorlage eine Kontosynchronisierung. Wenn das Konto vor dieser Aktualisierung bisher nicht an der Kontosynchronisierung mit anderen Kontovorlagen beteiligt war, ist dies evtl. auch nach der Aktualisierung der Fall.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole an.
2. Wählen Sie "Benutzer", "Synchronisierung", "Synchronisierung der Kontovorlage überprüfen".
3. Wählen Sie einen Benutzer aus.

   Ein Fenster mit den erwarteten, zusätzlichen und fehlenden Konten wird angezeigt.
4. Klicken Sie auf "Synchronisieren", um die Konten an die Vorlage anzupassen.
   a. Sie können ein Kontrollkästchen aktivieren, um das Konto auf dem Endpunkt zu erstellen. Wenn mehr als eine Kontovorlage für den Benutzer das gleiche Konto vorschreibt, wird das Konto durch das Zusammenführen aller relevanten Kontovorlagen erstellt.

      Dieses Konto wird den Kontovorlagen zugewiesen, die gegenwärtig nicht mit dem Konto synchronisiert sind. Kontosynchronisierung ist auf neu erstellten Konten nicht notwendig.

   b. Sie können ein Kontrollkästchen aktivieren, um zusätzliche Konten zu löschen. Allerdings können Benutzer berechtigte Gründe für den Besitz dieser Konten haben. Lassen Sie diese Option dann deaktiviert.

      Auf gewissen Endpunkten ist die Kontolöschungsfunktion deaktiviert; daher wird das Konto nicht gelöscht.

Synchronisieren von Endpunkt-Benutzerkonten mit Kontovorlagen

Diese Aufgabe synchronisiert ein Endpunkt-Benutzerkonto nach der Änderung einer zugeordneten Kontovorlage. Zum Beispiel enthält ein Active Directory-Konto möglicherweise keine Gruppen, aber die zugeordnete Kontovorlage ist dafür definiert, Gruppen zu enthalten.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole an.
2. Wählen Sie "Endpunkte", "Endpunkte verwalten", "Synchronisierung der Endpunktkonten überprüfen".
3. Wählen Sie einen Endpunkt aus.

   Ein Fenster wird angezeigt, das außer Konten auf diesem Endpunkt und zugeordneten Kontovorlagen anzeigt, welche Attribute nicht synchronisiert wurden.
4. Klicken Sie auf "Synchronisieren", um die Attribute für diese Konten an die Definition in der Kontovorlage anzupassen.

   Änderungen, die Sie an Kontovorlagen vornehmen, wirken sich folgendermaßen auf bestehende Konten aus:

   - Wenn Sie den Wert eines Funktionsattributs ändern, wird das entsprechende Kontoattribut aktualisiert, damit die Übereinstimmung mit dem Kontovorlagen-Attributwert sichergestellt ist. Weitere Informationen hierzu finden Sie in der Beschreibung von schwacher und starker Synchronisierung.
   - Bei bestimmten Kontoattributen wird vom Connector festgelegt, dass sie bei einer Kontovorlagen-Änderung nicht aktualisiert werden sollen. Beispiele sind bestimmte Attribute, deren Festlegung der Endpunkttyp nur während der Kontoerstellung zulässt, und das Kennwort-Attribut.

Synchronisierung von Funktionsattributen

Wenn Sie Funktionsattribute in einer Kontovorlage ändern, ändern sich ggf. auch die entsprechenden Attribute in den Konten. Ob die Attribute eines jeweiligen Kontos betroffen sind, ist von zwei Faktoren abhängig:

- ob die Kontovorlage für die Verwendung schwacher oder starker Synchronisierung definiert ist
- ob das Konto mehreren Kontovorlagen zugeordnet ist

Schwache Synchronisierung

Schwache Synchronisierung stellt sicher, dass Benutzer über das Mindestmaß an Funktionsattributen verfügen, das ihre Konten aufweisen sollten. Schwache Synchronisierung ist der Standard für die meisten Endpunkttypen. Wenn Sie eine Vorlage aktualisieren, die schwache Synchronisation verwendet, aktualisiert CA IdentityMinder Funktionsattribute folgendermaßen:

- Wenn ein numerisches Feld in einer Kontovorlage aktualisiert wird und der neue Zahlenwert höher als der im Konto vorhandene Wert ist, übernimmt CA IdentityMinder den neuen Wert für das Konto.
- Wenn bei einer Kontovorlage das Kontrollkästchen nicht ausgewählt war und Sie es nachträglich auswählen, aktualisiert CA IdentityMinder das Kontrollkästchen bei allen Konten, bei denen es nicht ausgewählt ist.
- Wenn eine Liste in einer Kontovorlage geändert wird, aktualisiert CA IdentityMinder alle Konten dahin gehend, dass neue Werte in der Liste, die in der im Konto vorhandenen Liste nicht vorhanden sind, hinzugefügt werden.

Falls ein Konto anderen Kontovorlagen zugeordnet ist (unabhängig davon, ob die entsprechenden Vorlagen schwache oder starke Synchronisierung nutzen), berücksichtigt CA IdentityMinder nur die geänderte Vorlage. Diese Aktion ist effizienter als eine Überprüfung aller Kontovorlagen. Da bei der schwachen Synchronisierung nur Funktionalitäten zu Konten hinzugefügt werden, ist es in der Regel nicht erforderlich, die anderen Kontovorlagen zu überprüfen.

Hinweis: Bei der Propagierung auf der Grundlage einer Kontovorlage mit schwacher Synchronisierung werden Änderungen, bei denen Funktionalitäten entfernt oder eingeschränkt werden, möglicherweise für einige Konten nicht übernommen. Denken Sie daran, dass bei Verwendung schwacher Synchronisierung niemals Funktionalitäten entfernt oder eingeschränkt werden. Wenn keine weiteren Vorlagen für ein Konto geprüft werden, kann bei der Propagierung nicht berücksichtigt werden, ob eine schwache Synchronisierung ausreicht.

Verwenden Sie in dieser Situation "Benutzer mit Kontovorlagen synchronisieren", um das Konto mit den zugehörigen Kontovorlagen zu synchronisieren.

Starke Synchronisierung

Eine starke Synchronisierung stellt sicher, dass Konten genau die in der Kontovorlage angegebenen Kontoattribute aufweisen.

Beispiel: Sie fügen eine Gruppe zu einer vorhandenen UNIX-Kontovorlage hinzu. Ursprünglich generierte die Kontovorlage Kontenmitglieder der Gruppe "Mitarbeiter". Jetzt möchten Sie Kontenmitglieder für die Gruppen "Mitarbeiter" und "System" generieren. Alle der Kontovorlage zugeordneten Konten werden als synchronisiert betrachtet, wenn jedes Konto Mitglied der Gruppen "Mitarbeiter" und "System" ist (und keiner anderen Gruppen). Konten, die nicht zur Gruppe "Mitarbeiter" gehören, werden beiden Gruppen hinzugefügt.

Folgende andere Faktoren müssen u. a. berücksichtigt werden:

- Wenn die Kontovorlage die starke Synchronisierung verwendet, werden Konten, die zu anderen Gruppen gehören als "Mitarbeiter" und "System", aus diesen zusätzlichen Gruppen entfernt.
- Wenn die Kontovorlage die schwache Synchronisierung verwendet, werden die Konten den Gruppen "Mitarbeiter" und "System" hinzugefügt. Jedes Konto, für das zusätzliche Gruppen definiert sind, bleibt Mitglied dieser Gruppen.

Hinweis: Synchronisieren Sie Konten regelmäßig mit den entsprechenden Vorlagen, um sicherzustellen, dass sie synchronisiert bleiben.

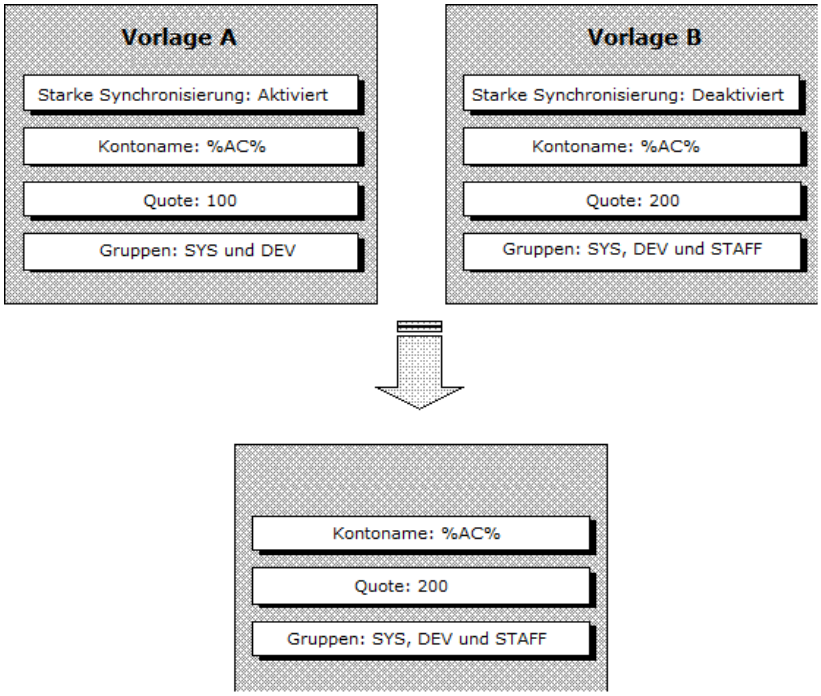
Konten mit mehreren Vorlagen

Die Synchronisierung hängt auch davon ab, ob das Konto zu mehr als einer Kontovorlage gehört. Wenn ein Konto nur eine Kontovorlage aufweist und diese Vorlage die starke Synchronisierung verwendet, wird jedes Attribut aktualisiert, um genau mit dem Kontovorlage-Attributwert übereinzustimmen. Das Ergebnis entspricht dem eines anfänglichen Attributs.

Ein Konto kann zu mehreren Kontovorlagen gehören, beispielsweise wenn ein globaler Benutzer zu mehreren Bereitstellungsrollen gehört, von denen jede ein bestimmtes Maß an Zugriff auf denselben verwalteten Endpunkt vorschreibt. In diesem Fall kombiniert CA IdentityMinder diese Kontovorlagen in einer gültigen Kontovorlage, die die Obermenge an Funktionen aus den einzelnen Kontovorlagen vorschreibt. Diese Kontovorlage verwendet die schwache Synchronisierung, wenn alle einzelnen Kontovorlagen diese Synchronisierung verwenden, oder die starke Synchronisierung, wenn eine der Kontovorlagen diese Synchronisierung verwendet.

Hinweis: In der Regel verwenden Sie entweder die schwache oder starke Synchronisierung für die Kontovorlagen für ein Konto, je nach dem, ob Ihre Unternehmensrollen den Zugriff, den Ihre Benutzer benötigen, komplett definieren. Wenn Ihren Benutzer keine klaren Rollen zugeordnet werden können und Sie den Konten Ihrer Benutzer zusätzliche Funktionen gewähren müssen, verwenden Sie die schwache Synchronisierung. Wenn Sie Rollen definieren können, um genau den Zugriff anzugeben, den Ihre Benutzer benötigen, verwenden Sie die starke Synchronisierung.

Das folgende Beispiel demonstriert, wie mehrere Kontovorlagen in einer einzelnen gültigen Kontovorlage kombiniert werden. In diesem Beispiel wird für eine Kontovorlage die schwache Synchronisierung und die andere Vorlage die starke Synchronisierung festgelegt. Daher wird die gültige Kontovorlage (eine Kombination aus den beiden Kontovorlagen) als Kontovorlage mit starker Synchronisierung behandelt. Das Attribut "Kontingent" (Ganzzahl) übernimmt den größeren Wert aus den beiden Kontovorlagen und das Attribut "Gruppen" (mehrwertig) übernimmt beide Werte aus den Richtlinien.



Attribute, mit denen nur neue Konten versehen werden

Bestimmte Attribute einer Kontovorlage werden nur bei der Erstellung eines Kontos angewendet. So ist beispielsweise das Kennwort-Attribut ein Regelausdruck, der das Kennwort für neue Konten definiert. Dieser Regelausdruck aktualisiert niemals das Kennwort eines Kontos. Änderungen hinsichtlich des Kennwort-Regelausdrucks betreffen nur nach dem Festlegen des Regelausdrucks erstellte Konten.

In ähnlicher Weise betrifft ein Vorlagen-Regelausdruck für ein schreibgeschütztes Kontoattribut nur Konten, die nach dem Festlegen dieses Regelausdrucks erstellt werden. Eine Änderung dieses Ausdrucks hat keine Auswirkungen auf vorhandene Konten.

Umgekehrte Synchronisierung mit Endpunktkonten

Obwohl das Erstellen, Löschen und Ändern von Konten in der Verantwortung von CA IdentityMinder liegt, lässt es sich nicht verhindern, dass ein Benutzer eines Endpunkt-Systems diese Vorgänge selbst ausführt. Diese Situation kann in Notfällen oder aufgrund bösartiger Absichten, z. B. bei Hackerangriffen, auftreten. Die umgekehrte Synchronisierung gewährleistet die Kontrolle über die Konten, die ein Benutzer auf jedem Endpunkt besitzt, indem Diskrepanzen zwischen CA IdentityMinder-Konten und Konten auf den Endpunkten identifiziert werden.

Wenn ein Konto beispielsweise mit Hilfe eines externen Tools in der Active Directory-Domäne erstellt wurde, muss CA IdentityMinder dieses potenzielle Sicherheitsrisiko erkennen. Darüber hinaus hat das Umgehen von CA IdentityMinder ein Fehlen von Genehmigungsprozessen und Audit-Berichten zur Folge.

Dies sind zwei Typen von Diskrepanz zwischen CA IdentityMinder und verwalteten Endpunkten:

- Ein neues Konto, das erkannt wurde
- Eine Änderung innerhalb eines vorhandenen Kontos

Sie können in beiden Fällen Richtlinien zur Behandlung der Änderung definieren. Anschließend lösen Sie die Ausführung von Richtlinien aus, indem Sie "Durchsuchen und Korrelieren" zum Aktualisieren von CA IdentityMinder verwenden.

Funktionsweise der umgekehrten Synchronisierung

Die umgekehrte Synchronisierung mit Endpunktkonten findet wie folgt statt:

1. Ein Administrator oder ein bösartiger Benutzer erstellt oder ändert ein Konto auf einem Endpunkt.
2. Wenn "Durchsuchen und Korrelieren" auf dem betreffenden Endpunkt ausgeführt wird, wird das neue oder geänderte Konto erkannt.
3. Der Bereitstellungsserver sendet eine Benachrichtigung an den CA IdentityMinder-Server.
4. Der CA IdentityMinder-Server sucht nach einer Richtlinie für die umgekehrte Synchronisierung, die mit der Änderung auf dem Endpunkt übereinstimmt.
5. Wenn eine übereinstimmende Richtlinie gefunden wird, wird sie ausgeführt. Wenn mehrere Richtlinien für das betreffende Konto gelten und diese Richtlinien denselben Bereich besitzen, wird die Richtlinie mit der höchsten Priorität ausgeführt.
6. Abhängig von der Richtlinie wird eine der folgenden Aktionen ausgeführt:
   - Bei einem neuen Konto akzeptiert, löscht oder deaktiviert die Richtlinie das Konto oder sendet es zur Workflow-Genehmigung.
   - Bei einem geänderten Konto akzeptiert die Richtlinie den Wert, setzt ihn auf den letzten bekannten Wert zurück oder sendet ihn zur Workflow-Genehmigung.
7. Wenn ein Workflow ausgewählt ist, wird ein neues Ereignis für den Workflow generiert, und die Genehmiger werden festgelegt. Anschließend wird eine der folgenden Aktionen ausgeführt:
   - Bei einem neuen Konto kann der Genehmiger das Konto akzeptieren, löschen, deaktivieren oder einen Benutzer zuweisen.
   - Bei einem geänderten Konto ist der Workflow-Prozess derselbe wie bei Wertänderungen in der Benutzerkonsole, abgesehen davon, dass abgelehnte Werte am Endpunkt zurückgesetzt werden.

Zuordnen von Endpunktattributen

Jedes Attribut für ein Endpunktkonto, das Sie mit der umgekehrten Synchronisierung verwalten möchten, muss einem globalen Benutzerattribut zugeordnet sein. Die meisten anfänglichen Benutzerprofilattribute, z. B. Kontoname, Kennwort und Kontostatus, sind standardmäßig zugeordnet. Andere Attribute, wie z. B. Funktionsattribute, sind jedoch nicht zugeordnet.

So ordnen Sie Endpunktattribute für die umgekehrte Synchronisierung zu:

1. Führen Sie in der Benutzerkonsole folgende Schritte aus:
   a. Klicken Sie auf "Endpunkte", "Endpunkt ändern".
   b. Suchen Sie nach einem Endpunkt, der die umgekehrte Synchronisierung benötigt, und wählen Sie diesen aus.
   c. Klicken Sie auf die Registerkarte "Attributzuordnung".
   d. Wählen Sie "Benutzerdefinierte Einstellungen verwenden" aus.
   e. Klicken Sie auf "Set Default" (Standard festlegen), um Standardeinstellungen wieder zur Liste hinzuzufügen.
   f. Klicken Sie auf "Hinzufügen", um ein neues benutzerdefiniertes Attribut hinzuzufügen.
   g. Wählen Sie ein verfügbares benutzerdefiniertes Attribut aus. Verwenden Sie beispielsweise "CustomField 10", wenn es in Ihrer Umgebung nicht zugeordnet ist.
   h. Ordnen Sie das benutzerdefinierte Attribut dem Namen des Kontoattributs zu, das Sie verwalten möchten.
   i. Klicken Sie auf "OK".
   j. Wiederholen Sie die Schritte f bis i, um Zuordnungen zwischen allen erforderlichen Kontoattributen und dem ausgewählten benutzerdefinierten Attribut hinzuzufügen.

      Sie können für alle Attribute, die Sie verwalten möchten, dasselbe benutzerdefinierte Attribut (in unserem Beispiel "CustomField 10") verwenden.
   k. Klicken Sie auf "OK".
2. Deaktivieren Sie im Bereitstellungs-Manager die eingehende Benachrichtigung wie folgt:
   a. Klicken Sie auf "System", "Domain configuration" (Domänenkonfiguration), "CA IdentityMinder-Server", "Enable Notification" (Benachrichtigung aktivieren).
   b. Wählen Sie "Nein" aus.
   c. Starten Sie den Bereitstellungsserver neu, um sicherzustellen, dass die Änderung wirksam wird.

Wichtig! Durch das Deaktivieren der eingehenden Benachrichtigung werden unnötige Benachrichtigungen während des Vorgangs zum Durchsuchen und Korrelieren vermieden. Anderenfalls würde jedes Konto, das für die neuen Attribute Werte besitzt, eine Benachrichtigung generieren.

3. Klicken Sie in der Benutzerkonsole auf "Endpunkte", "Durchsuchen und Korrelieren ausführen".
4. Wählen Sie eine Definition zum Durchsuchen und Korrelieren aus, bei der die Korrelation nicht ausgewählt ist.

   Durch diese Aktion werden die Benutzerspeicherattribute mit den neuen Endpunktattributdaten ausgefüllt. Bei großen Endpunkten kann diese Aufgabe einige Zeit in Anspruch nehmen.
5. Aktivieren Sie erneut die eingehende Benachrichtigung im Bereitstellungs-Manager.

Bei der nächsten Ausführung von "Durchsuchen und Korrelieren" für den betreffenden Endpunkt werden Kontoänderungsbenachrichtigungen generiert. Benachrichtigungen werden generiert, wenn eine Änderung für ein Attribut stattgefunden hat, das einem globalen Benutzerattribut zugeordnet ist, und eine Richtlinie für dieses Attribut wirksam ist.

Weitere Informationen:

Funktions- und anfängliche Attribute (siehe Seite 230)

Richtlinien für die umgekehrte Synchronisierung

Wenn ein Konto auf einem Endpunkt erstellt oder geändert wird, können Richtlinien für die umgekehrte Synchronisierung als Reaktion darauf entsprechende Aktionen durchführen. Beispielsweise erstellt ein Benutzer in verschiedenen Organisationseinheiten in der Unternehmensdomäne mehrere Active Directory-Konten. Darüber hinaus ändert der Benutzer einige Microsoft Exchange-Konten. Sie können mit Hilfe von Kontorichtlinien für die umgekehrte Synchronisierung die neuen und geänderten Konten ermitteln und entsprechende Aktionen als Reaktion bereitstellen.

Mit Hilfe der umgekehrten Synchronisierung können Sie Folgendes ausführen:

- Konfigurieren einer Richtlinie, um das neue Konto zu akzeptieren, abzulehnen oder zur Workflow-Genehmigung zu senden.
- Konfigurieren einer Richtlinie, um eine Änderung an einem Attribut zu akzeptieren, das ursprüngliche Attribut wiederherzustellen oder das Attribut zur Workflow-Genehmigung zu senden.
- Wenn ein Konto zur Workflow-Genehmigung gesendet wird, kann der Genehmiger eine der folgenden Aktionen durchführen:
  - Es ablehnen (es vom Endpunkt löschen/deaktivieren oder den Wert in den CA IdentityMinder-Benutzerspeicherwert ändern)
  - Es akzeptieren und den CA IdentityMinder-Benutzerspeicher aktualisieren, so dass er mit dem Konto übereinstimmt
  - Es einem Benutzer in der Benutzerkonsole zuweisen (bei einer Kontoerstellung)

Erstellen einer Richtlinie für neue Konten

Wenn Sie einen Prozess für den Fall der Erkennung eines neuen Kontos auf einem Endpunkt definieren möchten, erstellen Sie eine Kontorichtlinie, die für neue Konten gilt. Richtlinien für neue Konten werden ausgeführt, wenn Konten bei der Einbeziehung der Option zum Korrelieren in die Definition "Durchsuchen und Korrelieren" erkannt werden. Wenn ein Konto bei der alleinigen Ausführung von "Durchsuchen" gefunden wurde, wird die Richtlinie beim nächsten Mal ausgeführt, wenn die Option zum Korrelieren beim Durchsuchen des betreffenden Endpunkts einbezogen wird.

So erstellen Sie eine Richtlinie für neue Konten:

1. Klicken Sie in der Benutzerkonsole auf "Endpunkte", "Neu umkehren", "Richtlinie für neues Konto durch umgekehrte Synchronisierung erstellen".
2. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein.
3. Geben Sie folgende Parameter ein:
   - Priorität - Die Priorität der Richtlinie. Die Richtlinie mit der höchsten Priorität besitzt die niedrigste Nummer. Falls zwei Richtlinien dieselbe Priorität und denselben Bereich aufweisen, kann entweder die eine oder die andere ausgeführt werden. Stellen Sie daher sicher, dass Sie unterschiedliche Prioritätsstufen festlegen.
   - Endpunkttyp - Alle Endpunkte oder ein spezieller Endpunkttyp.
   - Endpunkt - Der Name des speziellen Endpunkts. Falls der Endpunkttyp den Wert "Alle" aufweist, ist die Auswahl auf "Alle Endpunkte" beschränkt.
   - Container - Der Container, in dem sich das Konto befindet. Dieses Feld gilt nur für hierarchische Endpunkte. Geben Sie den Container als Liste von Knoten ein, wobei Sie den Endpunkt als Letztes eingeben. Beispielsweise ist "untergeordnetes Element,übergeordnetes Element,Root" das korrekte Format für eine AD-Organisationseinheit mit dem Pfad "ou=untergeordnetes Element,ou=übergeordnetes Element,ou=Root,dc=Domäne,dc=Name".
   - Korrelierter Benutzer - Steuert, wann die Richtlinie ausgehend davon, ob im Bereitstellungsverzeichnis ein korrelierter Benutzer gefunden wird, ausgeführt werden soll.

4. Wählen Sie eine der folgenden Aktionen aus:
   - Akzeptieren - Für das Konto wird keine Aktion ausgeführt. Diese Aktion ist beispielsweise dann nützlich, wenn zwei Richtlinien vorhanden sind, von denen eine alle neuen Konten ablehnt und die andere, die eine höhere Priorität besitzt, Konten akzeptiert, die unter einer bestimmten Organisationseinheit erstellt wurden. Demzufolge würde ein unter dieser Organisationseinheit erstelltes Konto akzeptiert. Die ablehnende Richtlinie wird nicht ausgeführt, da sie eine geringere Priorität aufweist.
   - Löschen - Entfernt das Konto vom Endpunkt.
   - Deaktivieren - Das Konto verbleibt im Endpunkt, wird jedoch deaktiviert.
   - Zur Genehmigung senden - Sendet die Änderung zur Workflow-Genehmigung.
5. Führen Sie die folgenden Schritte aus, wenn Sie als Aktion "Zur Genehmigung senden" festlegen:
   a. Klicken Sie auf das Symbol neben "Workflow-Prozess".
   b. Wählen Sie einen Workflow-Prozess aus.
   c. Klicken Sie auf "OK".
6. Klicken Sie auf "Senden".

Wenn Sie der Richtlinie einen Workflow-Prozess zugewiesen haben, müssen Sie eine Genehmigungsaufgabe erstellen (siehe Seite 204).

Erstellen einer Richtlinie für geänderte Konten

Jedes Kontoattribut in einem Endpunktkonto kann durch die umgekehrte Synchronisierung verwaltet werden, solange es in der Attributzuordnung definiert (siehe Seite 197) ist.

Um einen Prozess für den Fall zu definieren, dass eine Diskrepanz zwischen vorhandenen Endpunktkonten und ihren bekannten Werten in CA IdentityMinder gefunden wird, können Sie eine Kontorichtlinie erstellen, die für vorhandene Konten gilt. Bei einem mehrwertigen Attribut können mehrere Werte hinzugefügt oder entfernt worden sein. In diesem Fall wird die Richtlinie separat auf jeden Wert angewendet, oder Sie können für verschiedene Werte unterschiedliche Richtlinien erstellen.

So erstellen Sie eine Richtlinie für geänderte Konten:

1. Klicken Sie in der Benutzerkonsole auf "Endpunkte", "Ändern umkehren", "Umgekehrte Synchronisierung - Richtlinie für geändertes Konto erstellen".
2. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein.
3. Geben Sie folgende Parameter ein:
   - Priorität - Die Priorität der Richtlinie. Die Richtlinie mit der höchsten Priorität besitzt die niedrigste Nummer. Falls zwei Richtlinien dieselbe Priorität und denselben Bereich aufweisen, kann entweder die eine oder die andere ausgeführt werden. Stellen Sie daher sicher, dass Sie unterschiedliche Prioritätsstufen festlegen.
   - Endpunkttyp - Alle Endpunkte oder ein spezieller Endpunkttyp.
   - Endpunkt - Der Name des speziellen Endpunkts. Falls der Endpunkttyp den Wert "Alle" aufweist, ist die Auswahl auf "Alle Endpunkte" beschränkt.
   - Container - Der Container, in dem sich das Konto befindet. Dieses Feld gilt nur für hierarchische Endpunkte. Geben Sie den Container als Liste von Knoten ein, wobei Sie den Endpunkt als Letztes eingeben. Beispielsweise ist "untergeordnetes Element,übergeordnetes Element,Root" das korrekte Format für eine AD-Organisationseinheit mit dem Pfad "ou=untergeordnetes Element,ou=übergeordnetes Element,ou=Root,dc=Domäne,dc=Name".
   - Attribut - Der physische Name.
   - Wert - Eine Zeichenfolgendarstellung des Wertes, die einen Stern (*****) als Platzhalter enthalten kann. Der Platzhalter steht für einen beliebigen Wert in der Änderung.

4. Wählen Sie eine der folgenden Aktionen aus:
   - Akzeptieren - Aktualisiert den Kontowert im CA IdentityMinder-Benutzerspeicher, damit dieser dem Wert im Endpunktkonto entspricht.
   - Ablehnen - Setzt das Attribut auf den ursprünglichen Wert zurück, ohne sich auf andere Änderungen an Attributen für das Konto auszuwirken.
   - Zur Genehmigung senden - Sendet die Änderung zur Workflow-Genehmigung.
5. Führen Sie die folgenden Schritte aus, wenn Sie als Aktion "Zur Genehmigung senden" festlegen:
   a. Klicken Sie auf das Symbol neben "Workflow-Prozess".
   b. Wählen Sie einen Workflow-Prozess aus.
   c. Klicken Sie auf "OK".
6. Klicken Sie auf "Senden".

Wenn Sie der Richtlinie einen Workflow-Prozess zugewiesen haben, müssen Sie eine Genehmigungsaufgabe erstellen (siehe Seite 204).

Erstellen einer Genehmigungsaufgabe für die umgekehrte Synchronisierung

Sie erstellen umgekehrte Genehmigungsaufgaben für Richtlinien, die eine "An Workflow senden"-Aktion besitzen. Beachten Sie bei der Erstellung der Aufgaben die folgenden Richtlinien:

- Für Aufgaben, die neue Konten genehmigen, haben Sie zwei Möglichkeiten.
  - Sie können ein generisches Genehmigungsfenster für Konten erstellen. Das Profilfenster für die Aufgabe zeigt nur allgemeine Informationen zu dem Konto an. Die Aufgabe "Umkehrung des neuen Kontos genehmigen" funktioniert auf diese Weise.
  - Wenn der Genehmiger die Details des neuen Kontos einsehen muss, muss das Fenster dem Endpunkttyp entsprechen. Daher sollte die Genehmigungsaufgabe mit dem Fenster nur für Richtlinien verwendet werden, die für diesen Endpunkttyp spezifisch sind. Die Aufgabe muss die Registerkarte "Genehmigung der Umkehrung" enthalten.
- Für Aufgaben, die Kontoänderungen genehmigen, muss das Genehmigungsfenster für einen Endpunkttyp spezifisch sein, so dass der Genehmiger die geänderten Werte sehen kann.

Umgekehrte Genehmigungsaufgaben sind identisch mit Genehmigungsaufgaben, die für Kontoänderungen verwendet werden. Wenn bereits eine Genehmigungsaufgabe für einen spezifischen Endpunkttyp vorhanden ist, kann diese Aufgabe verwendet werden. Für ein neues Konto ist eine zusätzliche Registerkarte "Genehmigung der Umkehrung" erforderlich. Falls noch keine Genehmigungsaufgabe für den Endpunkttyp vorhanden ist, gehen Sie wie folgt vor.

So erstellen Sie eine Genehmigungsaufgabe für die umgekehrte Synchronisierung:

1. Klicken Sie in der Benutzerkonsole auf "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe erstellen".
2. Wählen Sie die Aufgabe "Ändern" für den Endpunkt aus.

   Der Name enthält "ändern" und gibt den Namen des Endpunkttyps an. Beispiel: Active Directory-Konto ändern.
3. Nehmen Sie auf der Registerkarte "Profil" die folgenden Änderungen vor:
   - Ändern Sie den Namen der neuen Aufgabe.
   - Ändern Sie den Aufgaben-Tag.
   - Ändern Sie die Aktion in "Ereignis genehmigen".
4. Nehmen Sie auf der Registerkarte "Registerkarten" die folgenden Änderungen vor:
   a. Entfernen Sie alle Registerkarten "Beziehung".
   b. Fügen Sie die Registerkarte "Genehmigung der Umkehrung" hinzu, wenn die Aufgabe neue Konten genehmigen soll. Verschieben Sie diese Registerkarte an die Stelle der ersten Registerkarte.

5. Klicken Sie auf "Senden".
6. Wenn die Aufgabe dem Genehmigen neuer Konten dient, fügen Sie sie zu einer Rolle hinzu, zu der der Genehmiger gehören würde. Die Rolle definiert den Benutzerbereich, der für die Suche nach Benutzern verwendet wird, denen das neue Konto zugewiesen werden kann.

Ausführen der umgekehrten Synchronisierung

Die umgekehrte Synchronisierung findet statt, wenn Sie die Aufgabe Durchsuchen und Korrelieren ausführen verwenden. Mithilfe dieser Aufgabe aktualisieren Sie den CA IdentityMinder-Bereitstellungsspeicher mit den neuen oder geänderten Konten auf einem Endpunkt.

So führen Sie die umgekehrte Synchronisierung aus:

1. Erstellen Sie eine Definition "Durchsuchen und Korrelieren", die eine Option zum Korrelieren enthält. Die Korrelation ist zum Erkennen neuer Konten erforderlich.
2. Klicken Sie auf "Endpunkte", "Durchsuchen und Korrelieren ausführen".
3. Wählen Sie eine Definition aus, die für den Endpunkt mit den neuen oder geänderten Konten gilt.

   Hinweis: Bei der Korrelation mit dem vorhandenen Benutzer muss der Benutzer im Bereitstellungsverzeichnis vorhanden sein, anderenfalls wird der Benutzer mit dem Standardbenutzer in diesem Verzeichnis korreliert. Der CA IdentityMinder-Benutzerspeicher befindet sich nicht im Bereich der Aufgabe "Durchsuchen und Korrelieren".
4. Klicken Sie auf "Senden".

Wenn eine Richtlinie keinen Workflow-Prozess besitzt, werden die Konten bereits verarbeitet, wie in der Richtlinie definiert.

Hinweis: Wenn mehrere Attribute auf einem Konto abgelehnt wurden, das durch eine Richtlinie für die umgekehrte Synchronisierung erkannt wurde, werden alle Aktionen in ein Ereignis eingefügt. Falls dieses Ereignis jedoch aufgrund eines Problems mit einem der Attribute fehlschlägt, werden keine Attribute aktualisiert.

Wenn der Workflow Teil der Richtlinie ist, werden alle von der umgekehrten Synchronisierung generierten Genehmigungen für den Genehmiger unter "Workflow", "Meine Arbeitsliste anzeigen" angezeigt.

Für neue Konten hat der Genehmiger die folgenden Möglichkeiten:

- Der Genehmiger kann das Konto auf dem Endpunkt deaktivieren oder löschen, indem er "Löschen" oder "Deaktivieren" auswählt und anschließend auf "Ablehnen" klickt.
- Anderenfalls kann der Genehmiger das neue Konto akzeptieren, indem er auf "Bestätigen" klickt.

  Wenn ein Genehmiger im Feld "Korrelierter Benutzer" keinen Benutzer auswählt, wird das Konto dem Standardbenutzer zugewiesen. Wenn das Feld "Korrelierter Benutzer" in der Genehmigungsaufgabe ausgefüllt ist, wird das Konto mit diesem Benutzer korreliert. Das Feld "Korrelierter Benutzer" enthält den vorgeschlagenen Benutzer, der vom Korrelationsmechanismus gefunden wurde, sofern ein Benutzer gefunden werden kann.

Für geänderte Konten hat der Genehmiger die folgenden Möglichkeiten:

- Der Genehmiger sieht für jedes Konto, welche Werte geändert wurden, und kann diese Werte genehmigen oder ablehnen (genau wie bei in den Kontenverwaltungsfenstern initiierten Änderungen).
- Dem Genehmiger werden Änderungen an Funktionsattributen (z. B. Active Directory-Gruppen) als separate Genehmigungsereignisse angezeigt.

So überprüfen Sie, ob die umgekehrte Synchronisierung erfolgreich ausgeführt wurde:

1. Wechseln Sie zu "System", "Gesendete Aufgaben anzeigen".
2. Geben Sie Folgendes in das Feld "Aufgabenname" ein: "Bereitstellungsaktivität".
3. Klicken Sie auf Suchen.

Die Ergebnisse zeigen, ob die Ereignisse der umgekehrten Synchronisierung erfolgreich abgeschlossen wurden.

Erweitern der benutzerdefinierten Attribute an Endpunkten

Der Bereitstellungsserver kann benutzerdefinierte Endpunktattribute verwalten. Damit CA IdentityMinder benutzerdefinierte Endpunktattribute lesen kann, die mit Bereitstellungsrollen verbunden sind, müssen weitere Schritte durchgeführt werden.

So erweitern Sie die benutzerdefinierten Attribute an Endpunkten:

1. Generieren Sie Metadaten aus der Parser-Tabelle, wenn dieser Connector vor CA IdentityMinder r12.5 erstellt wurde.

   Weitere Informationen finden Sie im *Programmierhandbuch für Java Connector Server*.

2. Verwenden Sie Connector Xpress wie folgt:

   a. Installieren Sie die Metadaten im Namespace-Knoten.

   b. Generieren Sie eine JAR-Datei, Eigenschaftsdatei und Rollendefinitionsdatei mit Hilfe des Generators für Rollendefinitionen.

      Einzelheiten finden Sie im *Connector Xpress-Handbuch*.

3. Kopieren Sie die JAR-Datei in das folgende Verzeichnis:
   - (Windows) *app server home*/iam_im.ear/user_console.war/WEB-INF/lib
   - (UNIX) *app server home*\iam_im.ear\user_console.war\WEB-INF\lib

     Hinweis: Wenn Sie WebSphere verwenden, kopieren Sie die JAR-Datei nach: WebSphere_home/AppServer/profiles/*Profile_Name*/config/cells/*Cell_name*/applications/iam_im.ear/user_console.war/WEB-INF
4. Kopieren Sie die Eigenschaftsdatei in das folgende Verzeichnis:
   - (Windows) *app server home*/iam_im.ear/custom/provisioning/resourceBundles
   - (UNIX) *app server home*\iam_im.ear\custom\provisioning\resourceBundles

     Hinweis: Kopieren Sie für WebSphere die Eigenschaftendatei nach:

     WebSphere_home/AppServer/profiles/*Profile_Name*/config/cells/*cell_name*/applications/iam_im.ear\custom\provisioning\resourceBundles
5. Wiederholen Sie die beiden zuvor beschriebenen Schritte für jeden Knoten, wenn Sie einen Cluster haben.
6. Starten Sie den Anwendungsserver neu.
7. Importieren Sie die Rollendefinitionsdatei wie folgt:
   a. Wählen Sie in der Management-Konsole die Umgebung aus.
   b. Wählen Sie die Rollen- und Aufgabeneinstellungen aus.
   c. Klicken Sie auf "Importieren".
   d. Wählen Sie den Endpunkttyp aus und klicken Sie auf "Fertig stellen".

Kontoaufgaben

In der Benutzerkonsole können Sie Endpunktkonten erstellen, ändern, anzeigen oder löschen, die mit einem Identity Manager-Benutzer verbunden sind. Sie können auch andere Endpunktkonten zuweisen, die in CA IdentityMinder mit keinem Benutzer verbunden sind.

Es gibt vier Arten von Endpunktkonten:

Bereitgestellt

Konten, die erstellt werden, wenn dem Benutzer eine Bereitstellungsrolle zugewiesen wird

Exception

Konten, die erstellt werden, wenn dem Benutzer eine Kontovorlage zugewiesen wird

Verwaist

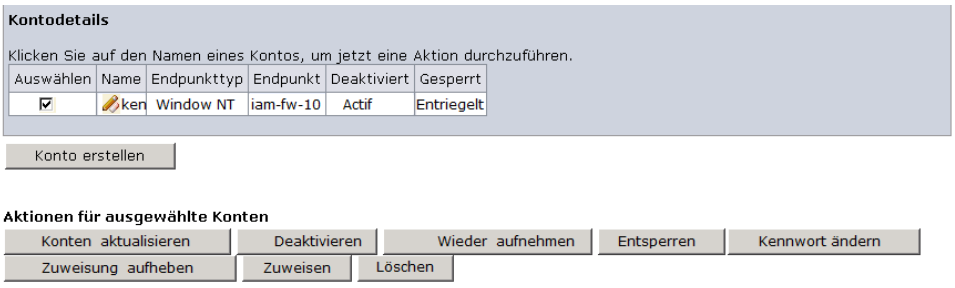
Konten, die auf dem Endpunktsystem erstellt werden und nicht mit einem CA IdentityMinder-Benutzer verknüpft sind

System

Konten, die auf einem Endpunktsystem erstellt wurden, nicht mit einem CA IdentityMinder-Benutzer verknüpft sind und zur Verwaltung des Endpunktsystems verwendet werden

Endpunktkonten anzeigen oder ändern

Aufgaben, die Ihnen erlauben, das Profil eines Benutzers anzuzeigen (wie "Benutzer anzeigen" oder "Mein Profil ändern") umfassen die Registerkarte "Konten", die die Endpunktkonten dieses Benutzers auflistet.



Für jedes Konto zeigt Identity Manager Informationen wie den Kontonamen, den Endpunkt des Kontos und den Status des Kontos an. Für eine Änderungsaufgabe sind zusätzliche Optionen verfügbar (Ändern des Kennworts eines Benutzers und Sperren oder Deaktivieren eines Kontos).

In diesem Beispiel umfasst die Registerkarte "Konten" die Schaltfläche "Suche". Das heißt, die Registerkarte ist mit einem Suchfenster konfiguriert. Sie können ein Listenfenster, ein Suchfenster oder beides für diese Registerkarte konfigurieren.

- Wenn beide Fenster konfiguriert werden, bestimmt das Suchfenster die Felder in den Suchergebnissen.
- Wenn nur ein Listenfenster konfiguriert wird, bestimmt dieses Fenster die Felder in den Suchergebnissen.
- Wenn kein Fenster konfiguriert wurde, verwendet die Registerkarte "Konten" eine statische Listenanzeige. Das bedeutet, dass die Registerkarte "Konten" nicht für Anzeigespalten angepasst werden kann.

Einzelheiten zu den weiteren Optionen, die Sie auf der Registerkarte "Konten" bereitstellen können, finden Sie in der Hilfe der Benutzerkonsole für die Registerkarte Konten konfigurieren.

Erstellen Sie ein bereitgestelltes Konto

Die empfohlene Methode, um ein Endpunktkonto für einen CA IdentityMinder-Benutzer zu erstellen, besteht in der Zuweisung einer Bereitstellungsrolle an den Benutzer. Der Benutzer erhält das Konto mit den Attributen, die in den Kontovorlagen für diese Rolle definiert sind. Falls erforderlich, wird das Endpunktkonto durch Änderungen an dieser Kontovorlage, z. B. die Postfachgröße für Exchange-Konten, aktualisiert.

So erstellen Sie ein bereitgestelltes Konto

1. Wählen Sie in der Benutzerkonsole die Befehle "Benutzer verwalten", "Benutzer ändern".
2. Wählen Sie einen Benutzer, der geändert werden soll.
3. Klicken Sie auf die Registerkarte "Bereitstellungsrollen".
4. Klicken Sie auf "Eine Bereitstellungsrolle hinzufügen".
5. Wählen Sie eine Rolle aus.
6. Klicken Sie auf "Submit".

Ausnahmenkonto erstellen

Wenn Sie "Benutzer ändern" auf einen Benutzer anwenden, können Sie direkt auf der Registerkarte "Konten" ein Konto erstellen. Bei diesem Konto handelt es sich um ein benanntes Ausnahmenkonto. Weil jedoch keine Bereitstellungsrolle im Zusammenhang mit diesem Konto steht, wird dieses Konto nicht aktualisiert, wenn Rollen mit Benutzern synchronisiert werden.

So erstellen Sie ein Ausnahmenkonto

1. Wählen Sie in der Benutzerkonsole die Befehle "Benutzer", "Endpunktkonten des Benutzers ändern".
2. Wählen Sie einen Benutzer, der geändert werden soll.
3. Klicken Sie auf "Erstellen".
4. Wählen Sie einen Endpunkt aus.
5. Wählen Sie einen Container aus, wenn einer für diesen Endpunkttyp erforderlich ist.
6. Füllen Sie die Felder auf jeder Registerkarte aus.
7. Klicken Sie auf "Submit".

Zuweisen von verwaisten Konten

Sie können in der Benutzerkonsole verwaiste Konten verwalten. Dabei handelt es sich um Konten, die keinem CA IdentityMinder-Benutzer zugeordnet sind.

So erstellen Sie einen Standardbenutzer für verwaiste Konten

Wenn das Bereitstellungsverzeichnis vom CA IdentityMinder-Benutzerspeicher getrennt ist, erstellen Sie den Standardbenutzer des Bereitstellungsservers im CA IdentityMinder-Benutzerspeicher. Der Standardbenutzer wird für verwaiste Konten verwendet.

1. Klicken Sie in der Benutzerkonsole auf die Registerkarte "Benutzer".
2. Klicken Sie auf "Benutzer verwalten", "Benutzer erstellen".
3. Geben Sie dem Benutzer den folgenden Namen, einschließlich der Klammern: `[Standardbenutzer]`

   Sie können nun Benutzern verwaiste Konten zuweisen.

So weisen Sie ein verwaistes Konto zu

1. Klicken Sie in der Benutzerkonsole auf "Endpunkte",
2. Klicken Sie auf "Verwaiste Konten verwalten".
3. Suchen Sie nach einem Benutzer und wählen diesen aus.
4. Klicken Sie auf einen Benutzer, der dem verwaisten Konto zugewiesen werden soll.

Zuweisen von Systemkonten

In der Benutzerkonsole können Sie Systemkonten verwalten. Dies sind Endpunkt-Benutzerkonten, die verwendet werden, um das Endpunktsystem zu verwalten.

Wenn Sie ein Systemkonto einem Benutzer zuweisen möchten, erstellen Sie eine Admin-Aufgabe, die auf der Aufgabe "Systemkonten verwalten" basiert. Die neue Aufgabe hat einen spezifischen CA IdentityMinder-Benutzer, der für einen spezifischen Endpunkt verantwortlich ist. Sie könnten eine Aufgabe für jeden Endpunkttyp erstellen.

So konfigurieren Sie eine Aufgabe, um Systemkonten zuzuweisen

1. Klicken Sie in der Benutzerkonsole auf "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe erstellen".
2. Wählen Sie als Basis für die neue Aufgabe "Systemkonten verwalten".

   Sie könnten z. B. eine Aufgabe mit der Bezeichnung *Oracle-Systemkonten verwalten* erstellen, um Systemkonten auf einem Oracle-Endpunkttyp zuzuweisen.

3. Klicken Sie auf der Registerkarte "Suchen" auf die Schaltfläche "Durchsuchen", um das Suchfenster zu bearbeiten. In diesem Fenster definieren Sie einen Suchfilter für einen Benutzer, der diesem Systemkonto zugewiesen werden soll.
4. Senden Sie die Aufgabe.
5. Fügen Sie diese Aufgabe in eine Rolle ein.
6. Weisen Sie die Rolle einem Benutzer zu, der Systemkonten für einen Endpunkt einem Benutzer zuweisen soll.

   Der Benutzer mit dieser Rolle kann die neue Aufgabe ausführen, um Systembenutzer einem CA IdentityMinder-Benutzer zuzuweisen.

Aufgabenfenster "Konto verschieben"

In diesem Aufgabenfenster können Sie Konten aus einem Container an einem Endpunkt in einen anderen Container verschieben. Dieses Fenster enthält folgende Felder:

Kontodetails verschieben

Gibt das Konto, den übergeordneten Container, den Zielcontainer, den Endpunkt und den Endpunkttyp für den Verschiebevorgang an.

Schaltfläche "Container auswählen"

Klicken Sie auf diese Schaltfläche, um nach verfügbaren Konto-Containern zu suchen, die zu dem Endpunkt gehören.

Löschen eines Endpunktkontos

Sie haben zwei Möglichkeiten, um ein Endpunktkonto zu löschen:

1. Mit Hilfe der Aufgabe "Benutzer ändern" auf der Registerkarte "Bereitstellungsrollen" entfernen Sie die Rolle, die das Konto erstellt hat.
2. Löschen Sie das Konto mit Hilfe der Aufgabe "Endpunktkonten des Benutzers ändern".

So löschen Sie ein Konto mit Hilfe von "Endpunktkonten des Benutzers ändern"

1. Wählen Sie in der Benutzerkonsole die Befehle "Benutzer", "Endpunktkonten des Benutzers ändern".
2. Wählen Sie einen Benutzer, der geändert werden soll.
3. Suchen Sie nach Konten auf Grundlage eines Endpunkttyps.
4. Wählen Sie ein Konto.
5. Klicken Sie auf die Schaltfläche Löschen.

Gelöschte Konten werden erneut erstellt, wenn Sie den Bereitstellungs-Manager wie folgt verwenden:

- "Benutzer mit Rollen synchronisieren" erstellt bereitgestellte Konten erneut, Konten, die erstellt wurden, wenn ein Benutzer eine Bereitstellungsrolle hat.
- "Konten mit Kontovorlagen synchronisieren" erstellt Ausnahmen (wenn das Konto eine Kontovorlage hat) und bereitgestellte Konten erneut.

Ändern des Kennworts für ein Endpunktkonto

Sie können das Kennwort eines Endpunktkontos ändern, ohne das aktuelle Kennwort zu kennen.

So ändern Sie das Kennwort eines Endpunktkontos

1. Wählen Sie in der Benutzerkonsole die Befehle "Benutzer", "Endpunktkonten des Benutzers ändern".
2. Wählen Sie einen Benutzer, der geändert werden soll.
3. Suchen Sie nach Konten auf Grundlage eines Endpunkttyps.
4. Wählen Sie ein oder mehrere Konten aus.
5. Klicken Sie auf die Schaltfläche "Kennwort ändern".
6. Geben Sie ein neues Kennwort ein.

   Das neue Kennwort wird anhand der Kennwortrichtlinie von CA IdentityMinder überprüft.
7. Klicken Sie auf "Submit".

Durchführen von Aktionen auf mehrere Konten

Sie können mehrere andere Aktionen auf ein oder mehrere Konten ausführen. Sie können z. B. ein deaktiviertes Konto wieder aufnehmen, ein Konto entsperren, wenn ein Benutzer das falsche Kennwort eingegeben hat oder ein Konto einem Benutzer zuweisen bzw. eine Kontozuweisung aufheben. Die Aktionen gelten für alle ausgewählten Konten und das Verfahren ist dasselbe.

So führen Sie Aufgaben auf mehrere Konten aus

1. Wählen Sie in der Benutzerkonsole die Befehle "Benutzer", "Endpunktkonten des Benutzers ändern".
2. Wählen Sie einen Benutzer, der geändert werden soll.
3. Suchen Sie nach Konten auf Grundlage eines Endpunkttyps.
4. Wählen Sie ein oder mehrere Konten aus.
5. Klicken Sie auf eine beliebige Schaltfläche unter "Aktionen für ausgewählte Konten".
6. Nehmen Sie die Eingaben im daraufhin angezeigten Dialogfeld vor, und klicken Sie auf "Senden".

Erweiterte Kontovorgänge

Im Bereitstellungsmanager können Sie verschiedene zusätzliche Vorgänge für Konten ausführen:

- Zuordnen von Konten zu anderen globalen Benutzern
- Automatische Durchsuchung von Konten
- Löschen von Konten
- Verwenden von "Löschen steht aus"
- Wiederherstellen von gelöschten Konten

Ändern des globalen Benutzers für ein Konto

Nachfolgend finden Sie Beispiele für Situationen, in denen ein Konto einem anderen globalen Benutzer zugeordnet werden soll:

- Zwei globale Benutzer haben denselben Namen, und CA IdentityMinder korreliert das Konto mit der falschen Person.
- CA IdentityMinder hat ein Konto mit dem [Standardbenutzer]-Objekt korreliert, und Sie möchten es einem anderen globalen Benutzerobjekt zuordnen.
- Sie haben ein Konto mit der Option "Neu" erstellt, und jetzt möchten Sie es einem globalen Benutzer zuordnen.

Um ein Konto einem anderen globalen Benutzer im Bereitstellungsmanager zuzuordnen, verschieben Sie das Konto per Drag & Drop zum richtigen globalen Benutzer.

Funktionsweise der automatischen Durchsuchung

Das Ergänzen oder Löschen von Konten oder anderen Objekten mithilfe von systemeigenen Tools des Endpunkts wird in CA IdentityMinder erst bemerkbar, wenn Sie den Endpunkt durchsuchen. Der Durchsuchungsprozess erkennt Ergänzungen und Löschungen (und in einigen Fällen Änderungen), die aufgetreten sind, und übernimmt diese Änderungen in der CA IdentityMinder-Darstellung des Objekts im Bereitstellungsverzeichnis.

Wenn Sie mit dem Bereitstellungsmanager jedoch versuchen, ein Objekt mit demselben Namen zu erstellen, bevor die Durchsuchung durchgeführt wird, erkennt CA IdentityMinder, dass ein Objekt mit diesem Namen bereits vorhanden ist, und meldet einen Fehler. CA IdentityMinder durchsucht dann dieses Objekt und erstellt eine Darstellung davon im Bereitstellungsverzeichnis. Sie können sofort anfangen, mit diesem Objekt zu arbeiten. Die automatische Durchsuchung eines Objekts tritt immer dann auf, wenn ein Vorgang zum Hinzufügen, Verschieben oder Umbenennen den Fehler, dass etwas bereits vorhanden ist, auf dem Endpunkt generiert, und wenn das Objekt nicht im Bereitstellungsverzeichnis vorhanden ist.

Sie können die automatische Durchsuchung mit dem Domänenkonfigurationsparameter für die Synchronisierung /automatische Korrelation verbinden, der im *Provisionierungs-Referenzhandbuch* beschrieben wird. Wenn diese Funktionen zusammen verwendet werden, führen sie zunächst einen Versuch durch, ein neues Konto zu erstellen, indem sie ein Konto aus einer Kontovorlage erstellen. Dann werden die folgenden Schritte durchgeführt:

- Erkennen eines nicht durchsuchten Kontos
- Automatisches Durchsuchen dieses Kontos
- Automatisches Korrelieren des Kontos mit dem globalen Benutzer
- Hinzufügen einer Kontovorlage zum Konto, als ob es ein vorhandenes mit diesem globalen Benutzer korreliertes Konto wäre

Löschen von Konten

Wenn Sie ein Konto löschen müssen, können Sie die folgenden Methoden im Bereitstellungsmanager verwenden:

- Klicken Sie mit der rechten Maustaste auf das Konto, und wählen Sie "Löschen" aus.
- Klicken Sie mit der rechten Maustaste auf einen globalen Benutzer, und wählen Sie "Benutzer löschen" und "Konten" aus.
- Führen Sie den Assistenten "Konten löschen" aus.
- Synchronisieren Sie globale Benutzer mit Bereitstellungsrollen, und geben Sie an, dass Sie zusätzliche Konten löschen möchten.

Wenn Sie einen globalen Benutzer aus einer Bereitstellungsrolle entfernen, bietet der Bereitstellungsmanager die folgenden Optionen zum Löschen von Konten:

- Wenn Sie beschließen, diese Konten zu löschen, entfernt CA IdentityMinder die Konten aus dem Bereitstellungsverzeichnis.
- Wenn Sie beschließen, die Konten nicht zu löschen, können Sie die Option "Benutzer mit Rollen synchronisieren " verwenden und "Konten löschen" auswählen.

Wenn Sie einen globalen Benutzer aus einer Bereitstellungsrolle entfernen, bevor Sie die Konten löschen, können Sie die Konten für den globalen Benutzer auflisten. Klicken Sie mit der rechten Maustaste auf den globalen Benutzer, und wählen Sie "List Accounts" (Konten auflisten) aus.

- Die Kontoauflistung zeigt für jedes Konto die Bereitstellungsrollen an, zu denen es gehört. Wenn ein Konto zu einer Bereitstellungsrolle gehört, wird es gelöscht, wenn Sie den entsprechenden Benutzer aus der Rolle entfernen und die Benutzersynchronisierungsaktion durchführen, mit der die Konten gelöscht werden.
- Wenn ein Konto zu keiner Bereitstellungsrolle gehört, handelt es sich dabei um ein zusätzliches Konto, und es wird bei der Überprüfung mit "Check User Synchronization" (Benutzersynchronisierung) gemeldet. Das Konto wird gelöscht, wenn Sie den Menüpunkt "Benutzer mit Rollen synchronisieren" für den globalen Benutzer auswählen.

Verwenden von "Löschen steht aus"

CA IdentityMinder kann so konfiguriert werden (für jeden Endpunkt spezifisch), dass Konten an einem Endpunkt nicht gelöscht werden, wenn Administratoren Lösch- oder Synchronisierungsaktionen initiieren, bei denen die Konten normalerweise gelöscht werden. Stattdessen werden die Konten in CA IdentityMinder in den Status "Löschen steht aus" und auf dem verwalteten Endpunkt in den Status "Deaktiviert" versetzt.

Konten mit dem Status "Löschen steht aus" können im Bereitstellungsmanager auf der Registerkarte "Statistiken" der Kontoeigenschaften identifiziert werden. Ein deaktiviertes Konto hat den Deaktivierungsgrund "Löschen steht aus" und einen Zeitstempel, der den Beginn dieses Status angibt. Werden der Status "Löschen steht aus" und der Deaktivierungs-Zeitstempel gespeichert, kann ein Hilfsprogramm geschrieben werden, das Konten mit dem Status "Löschen steht aus" identifiziert und auf dem Bereitstellungsserver und auf dem verwalteten Endpunkt löscht.

Wiederherstellen von gelöschten Konten

Wenn Sie zum Löschen eines Kontos an einem verwalteten Endpunkt ein anderes Tool als CA IdentityMinder verwenden, meldet die Funktion "Check Account Synchronization" (Kontosynchronisierung prüfen), dass das Konto fehlt, weil es im Bereitstellungsverzeichnis, aber nicht auf dem verwalteten Endpunkt vorhanden ist. Stellen Sie in dem Fall das Konto auf dem Endpunkt wieder her, indem Sie die Funktion "Konten mit Kontovorlage synchronisieren" ausführen, die das Konto mithilfe der dem Konto zugeordneten Kontovorlagen wiederherstellt.

Wenn Konten wiederhergestellt werden, werden sie in CA IdentityMinder als wiederhergestellte Konten protokolliert. Diese Konten können von aktualisierten Konten unterschieden werden, weil die Administratoren wissen müssen, dass Attribute, abgesehen von den Funktionsattributen (beispielsweise Kennwörter), auf die ursprünglichen Kontovorlagenwerte festgelegt worden sind.

Kapitel 9: Bereitstellungsrollen

Dieses Kapitel enthält folgende Themen:

Bereitstellungsrollen und Kontovorlagen (siehe Seite 219)
Erstellen von Rollen zum Zuweisen von Konten (siehe Seite 220)
Aufgaben im Zusammenhang mit Rollen und Vorlagen (siehe Seite 224)
Attribute in Kontovorlagen (siehe Seite 229)
Erweiterte Regelausdrücke (siehe Seite 233)
Leistung von Bereitstellungsrollen (siehe Seite 240)
Provisionierung von Aufgaben für vorhandene Umgebungen (siehe Seite 242)

Bereitstellungsrollen und Kontovorlagen

Zur Vereinfachung der Kontoverwaltung erstellen und pflegen Sie Konten mit Hilfe von Kontovorlagen, die in Bereitstellungsrollen verwendet werden. Eine Bereitstellungsrolle enthält eine oder mehrere Kontovorlagen. Wenn Sie eine solche Rolle auf einen Benutzer anwenden, stehen diesem Benutzer die Konten zur Verfügung, die durch die Vorlagen definiert werden.

Diese Vorlagen bilden die Grundlage für Konten auf einem spezifischen Endpunkttyp. Sie bieten dieselbe Art von Fähigkeiten wie Bereitstellungsrichtlinien in eTrust Admin.

Mit Hilfe von Kontovorlagen können Sie:

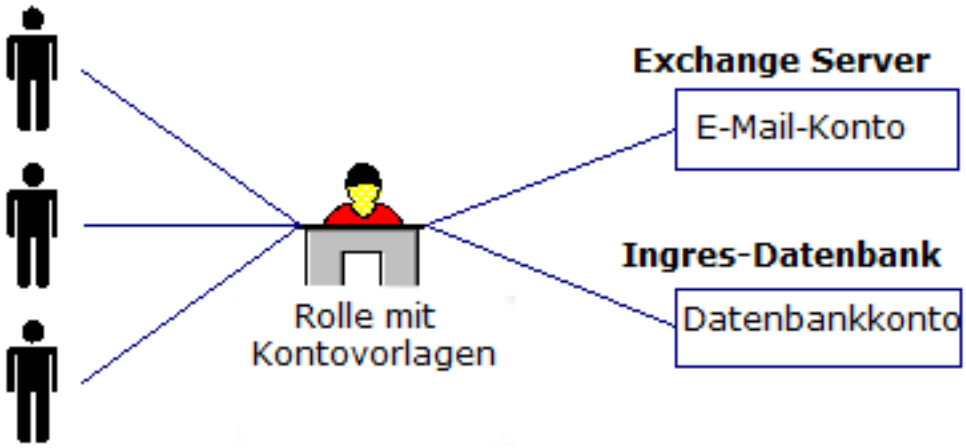
- steuern, über welche Kontoattribute Benutzer von CA IdentityMinder bei Erstellung ihrer Konten auf einem Endpunkt verfügen
- Attribute mit Hilfe von Regelzeichenfolgen oder Werten definieren
- Kontoattribute aus unterschiedlichen Bereitstellungsrollen kombinieren, wodurch Benutzer auf einem spezifischen Endpunkt nur ein einziges Konto mit allen erforderlichen Kontoattributen erhalten
- Kontoattribute erstellen und aktualisieren, wenn globale Benutzer Bereitstellungsrollen wechseln
- Kontoattribute synchronisieren, damit globale Benutzer nur die erforderlichen Attribute besitzen
- Abfragen durchführen, um festzustellen, welche Konten im Rahmen einer Synchronisierung erstellt, aktualisiert oder gelöscht werden sollten
- feststellen, welche Kontoattribute mit Hilfe von Bereitstellungsrollen synchronisiert werden können und welche nicht

Erstellen von Rollen zum Zuweisen von Konten

In den meisten Organisationen verbringen Administratoren bedeutende Zeit damit, Benutzern Anmeldungskonten für unterschiedliche Systeme und Anwendungen bereitzustellen. Um diese wiederholte Aktivität zu vereinfachen, können Sie Bereitstellungsrollen erstellen. Dies sind Rollen, die Kontovorlagen enthalten. Die Vorlagen definieren die Attribute, die in einem Kontotyp vorhanden sind. Zum Beispiel definiert eine Kontovorlage für ein Exchange-Konto Attribute wie die Größe des Postfachs. Kontovorlagen definieren auch, wie Benutzerattribute Konten zugeordnet werden.

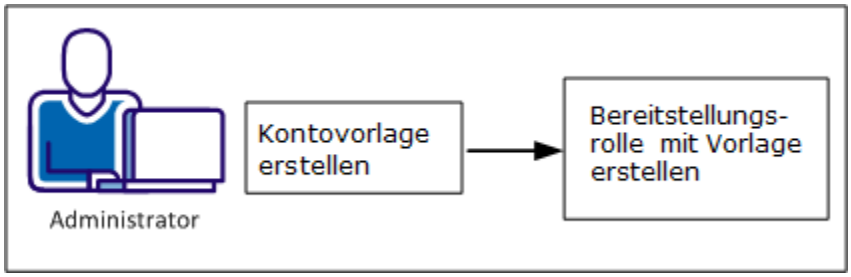
Betrachten Sie ein Beispiel, in dem jeder Mitarbeiter von Forward, Inc. Zugriff auf eine Datenbank und E-Mail benötigt. Ein Administrator will vermeiden, für jeden Mitarbeiter einzeln ein Datenbankkonto und ein E-Mail-Konto zu erstellen. Deswegen erstellt der Administrator eine Bereitstellungsrolle für dieses Unternehmen. Die Rolle enthält eine Kontovorlage für einen Microsoft Exchange-Server, um E-Mail-Konten bereitzustellen, und eine Vorlage für eine Oracle-Datenbank. In diesem Beispiel werden der Exchange-Server und die Oracle-Datenbank Endpunkte genannt. Dabei handelt es sich um das System oder die Anwendung, wo die Konten vorhanden sind.

Hinweis: Forward, Inc. ist ein fiktiver Unternehmensname, der ausschließlich als Beispiel dient und sich auf kein vorhandenes Unternehmen beziehen soll.



Nachdem die Rollen erstellt worden sind, können Geschäftsadministratoren, wie Manager oder Supportpersonal, diese Rollen Benutzern zuweisen, um ihnen Konten in Endpunkten zuzuweisen. Nachdem Benutzern die Rolle zugewiesen wurde, können sie sich beim Endpunkt anmelden.

Das Erstellen einer Bereitstellungsrolle, die eine Kontovorlage einschließt, ist ein zweistufiger Prozess:



Die folgenden Abschnitte erklären, wie Sie eine Rolle erstellen, mit der Konten zugewiesen werden können:

1. Kontovorlage erstellen (siehe Seite 222)
2. Erstellen einer Bereitstellungsrolle (siehe Seite 223)

Kontovorlage erstellen

Zur Vereinfachung der Kontoverwaltung erstellen und pflegen Sie Konten mit Hilfe von Kontovorlagen, die in Bereitstellungsrollen verwendet werden. Eine Bereitstellungsrolle enthält eine oder mehrere Kontovorlagen. Wenn Sie eine solche Rolle auf einen Benutzer anwenden, stehen diesem Benutzer die Konten zur Verfügung, die durch die Vorlagen definiert werden.

Diese Vorlagen bilden die Grundlage für Konten auf einem spezifischen Endpunkttyp.

Mit Hilfe von Kontovorlagen können Sie:

- Steuern, über welche Kontoattribute Benutzer bei Erstellung ihrer Konten auf einem Endpunkt verfügen
- Attribute mit Hilfe von Regelzeichenfolgen oder Werten definieren
- Kontoattribute aus unterschiedlichen Bereitstellungsrollen kombinieren, wodurch Benutzer auf einem spezifischen Endpunkt nur ein einziges Konto mit allen erforderlichen Kontoattributen erhalten
- Kontoattribute erstellen und aktualisieren, wenn globale Benutzer Bereitstellungsrollen wechseln

Mit dem CA IdentityMinder-Server wird für jeden Endpunkttyp eine Standardkontovorlage installiert. In einer Bereitstellungsrolle können Sie die Standardkontovorlage verwenden, oder Sie können für jeden konfigurierten Endpunkt eigene Kontovorlagen erstellen.

So erstellen Sie eine Kontovorlage

1. Wählen Sie "Endpunkt auswählen", "Kontovorlagen", "Kontovorlage erstellen".
2. Wählen Sie einen Endpunkttyp für die Vorlage aus.
3. Definieren Sie den Endpunktnamen als Systemnamen des Endpunkts oder gegebenenfalls als "localhost".
4. Wählen Sie die Endpunkte aus, die auf der Registerkarte "Endpunkte" verwendet werden sollen.
5. Füllen Sie die Felder in den Registerkarten aus, oder verwenden Sie die Standardwerte.

   Jeder Endpunkttyp verfügt über andere Registerkarten. Klicken Sie auf "Hilfe", um Informationen zu den Felddefinitionen anzuzeigen.
6. Klicken Sie auf "Senden".

Hinweis: Wenn bei der Suche nach Endpunktobjekten in der Kontovorlage mehr als ein Endpunkt angegeben wird, wird die gemeinsame Teilmenge (Schnittmenge) der zugehörigen Objekte zurückgegeben. Ein Beispiel ist eine Active Directory-Gruppe, die auf jedem der ausgewählten Endpunkte vorhanden ist, die der Kontovorlage zugeordnet sind. Wenn die Suchergebnisse andere Attribute als den Objektnamen enthalten, werden die Attributwerte der Objekte angezeigt, die dem ersten Endpunkt zugeordnet sind. Ein Beispiel ist das Beschreibungsattribut für das Sprachobjekt in einem PeopleSoft-Connector.

Erstellen einer Bereitstellungsrolle

Sie erstellen eine Bereitstellungsrolle, nachdem Sie die Rollenanforderungen festgelegt haben:

- Welche Benutzer benötigen andere Konten
- Welche Konten werden mit der Rolle verknüpft
- Wer sind die Mitglieder, Administratoren und Eigentümer der Rolle

So erstellen Sie eine Bereitstellungsrolle

1. Klicken Sie in der Benutzerkonsole zunächst auf die Option "Rollen und Aufgaben" und dann die Option "Bereitstellungsrollen" aus. Wählen Sie dann die Option "Bereitstellungsrolle erstellen" aus.

   Um Details zu jeder Registerkarte zu erhalten, klicken Sie auf die Hilfeverknüpfung in dem Fenster.

2. Vervollständigen Sie die Registerkarte "Profil". Nur das Feld "Name" muss einen Eintrag enthalten.

   Hinweis: Sie können auf der Registerkarte "Profil" benutzerdefinierte Attribute angeben, die weitere Informationen zu Bereitstellungsrollen enthalten. Sie können diese zusätzlichen Informationen verwenden, um Rollensuchvorgänge in Umgebungen zu erleichtern, die eine große Anzahl von Rollen enthalten.

3. Vervollständigen Sie die Registerkarte "Kontovorlagen".

   a. Klicken Sie auf einen Endpunkttyp wie z. B. ein ActiveDirectory.

   b. Klicken Sie auf eine Kontovorlage.

      Die Vorlagen, auf die Sie klicken können, basieren auf dem Endpunkttyp.

   c. Fügen Sie mehr Kontovorlagen hinzu, als für die verschiedenen Endpunkttypen benötigt werden.

4. Stellen Sie die Bereitstellungsrollen-Registerkarte fertig, wenn Sie Bereitstellungsrollen in dieser Registerkarte schachteln wollen.

   Dieser Schritt erfordert, dass Sie geschachtelte Rollen (siehe Seite 228) für diese Umgebung aktiviert haben.

5. Vervollständigen Sie die Registerkarte "Administratoren", indem Sie Admin-Regeln hinzufügen, die steuern, wer Mitglieder und Administratoren dieser Rolle verwaltet.

6. Vervollständigen Sie die Registerkarte "Eigentümer", indem Sie Eigentümerregeln hinzufügen, die steuern, wer diese Rolle ändern kann.

7. Klicken Sie auf "Senden".

8. Um zu überprüfen, ob die Rolle erstellt wurde, klicken Sie auf "Bereitstellungsrollen", "Bereitstellungsrolle anzeigen".

Aufgaben im Zusammenhang mit Rollen und Vorlagen

Sie können in der Benutzerkonsole Bereitstellungsrollen erstellen und verwalten, indem Sie "Rollen und Aufgaben" wählen und unterhalb von "Bereitstellungsrollen" eine Aufgabe auswählen. Die angebotenen Aufgaben umfassen Standardvorgänge, wie die Aufnahme eines Benutzers als Mitglied einer Rolle, das Ändern oder das Löschen einer Rolle.

Vor dem Erstellen einer Bereitstellungsrolle benötigen Sie eine Kontovorlage, die in die Rolle aufgenommen wird, oder eine Bereitstellungsrolle, die Sie importieren möchten. Sie können Rollen importieren, die im Bereitstellungs-Manager oder in eTrust Admin erstellt wurden. CA IdentityMinder unterstützt jedoch keine verschachtelten Rollen, die in eTrust Admin erstellt wurden.

Importieren einer Bereitstellungsrolle

Obwohl Sie Bereitstellungsrollen in der Benutzerkonsole verwalten, sind möglicherweise einige Bereitstellungsrollen im Bereitstellungs-Manager oder in einer externen Anwendung erstellt worden. Sie können für diese Bereitstellungsrollen den Besitzer der Rolle zurücksetzen und einen CA IdentityMinder-Administrator festlegen, um die Verwaltung über die Benutzerkonsole durchzuführen.

So importieren Sie eine Bereitstellungsrolle

1. Melden Sie sich bei der Benutzerkonsole als Benutzer mit der Rolle "System-Manager" an. Klicken Sie auf "Rollen und Aufgaben".

2. Klicken Sie zuerst auf die Option "Bereitstellungsrollen" und dann auf die Option "Bereitstellungsrollen-Eigentümer zurücksetzen". Wählen Sie dann eine Bereitstellungsrolle aus, die im Bereitstellungs-Manager erstellt wurde.

3. Vervollständigen Sie die Registerkarte "Eigentümer", indem Sie Eigentümerregeln hinzufügen, die steuern, wer diese Rolle ändern kann.
4. Klicken Sie auf "Submit".

Die Rolle kann jetzt mit Hilfe von Aufgaben in der Kategorie "Bereitstellungsrollen" geändert, zugewiesen oder angezeigt werden.

Zuweisen von neuen Eigentümern für Bereitstellungsrollen

Sie können eine oder mehrere Bereitstellungsrollen auswählen und ihnen Eigentümerrichtlinien zuweisen, um festzulegen, wer die Rollen ändern darf.

So weisen Sie neue Eigentümer für Bereitstellungsrollen zu

1. Melden Sie sich bei der Benutzerkonsole als Benutzer mit der Rolle "System-Manager" an.
2. Klicken Sie auf "Rollen und Aufgaben".
3. Klicken Sie auf "Bereitstellungsrollen", "Eigentümerrichtlinien für Bereitstellungsrollen erstellen".
4. Wählen Sie eine oder mehrere Bereitstellungsrollen aus.
5. Vervollständigen Sie die Registerkarte "Eigentümer", indem Sie Eigentümerregeln hinzufügen, die steuern, wer diese Rolle ändern kann.
6. Klicken Sie auf "Senden".

Benutzer, die die Richtlinien für neue Eigentümer erfüllen, können die ausgewählten Bereitstellungsrollen ändern.

Kennwörter für von Bereitstellungsrollen erstellte Konten

Wenn einem Benutzer eine Bereitstellungsrolle zugewiesen wird, schlägt die Kontoerstellung für diesen Benutzer fehl, wenn das Kennwort des CA IdentityMinder-Benutzers nicht den Kennwortanforderungen des Endpunkts entspricht. Diese Situation schließt das Erstellen eines neuen Benutzers mit einem temporären Kennwort ein.

Legen Sie die Kennwortrichtlinie daher so fest, dass sie mit den Anforderungen des Endpunktkennworts (oder strenger) übereinstimmt. Sie können die Kennwortrichtlinie mithilfe der CA IdentityMinder-Kennwortrichtlinie oder des bereitgestellten Kennwortprofils festlegen. Wenn beide Methoden verwendet werden, müssen die Richtlinien übereinstimmen.

Verarbeitungsreihenfolge von Ereignissen des Typs "Bereitstellungsrolle"

Einige Standardaufgaben in CA IdentityMinder enthalten *Ereignisse*. Dabei handelt es sich um Aktionen, die CA IdentityMinder durchführt, um eine Aufgabe abzuschließen, die die Bereitstellungsrollen-Mitgliedschaft festlegt. So gehört beispielsweise zu der Standardaufgabe "Benutzer ändern" die Ereignisse "AssignProvisioningRoleEvent" (dem Benutzer die Bereitstellungsrolle zuweisen) und "RevokeProvisioningRoleEvent" (Bereitstellungsrolle von Benutzer widerrufen). Das Zuweisen von Bereitstellungsrollen fügt einem Endpunkt ein Konto hinzu, das Widerrufen entfernt es wieder. In einigen Fällen verlangt der Endpunkt, dass alle Aktionen zum Hinzufügen vor den Aktionen zum Entfernen durchgeführt werden.

Um zu erzwingen, dass CA IdentityMinder Aktionen zum Hinzufügen als Erstes verarbeitet, aktivieren Sie in der Management-Konsole die Einstellung "Accumulation of Provisioning Role Membership Events" (Kumulierung der Bereitstellungsrollen-Mitgliedschaft-Ereignisse). Wenn diese Einstellung aktiviert ist, fasst CA IdentityMinder Aktionen zum Hinzufügen und Entfernen in einem einzelnen Ereignis zusammen, dem sogenannten AccumulatedProvisioningRolesEvent. Wenn beispielsweise die Aufgabe "Benutzer ändern" einen Benutzer drei Bereitstellungsrollen zuweist und ihn von zwei anderen entfernt, wird ein Ereignis vom Typ "AccumulatedProvisioningRolesEvent" generiert, das fünf Aktionen umfasst: drei Aktionen zum Hinzufügen sowie zwei weitere zum Entfernen.

Wird dieses Ereignis ausgeführt, werden alle Aktionen zum Hinzufügen zu einem einzelnen Vorgang zusammengefasst und zur Verarbeitung an den Bereitstellungsserver gesendet. Im Anschluss an die Verarbeitung dieser Hinzufügungsaktionen kombiniert CA IdentityMinder die Entfenrungsaktionen zu einem einzelnen Vorgang und sendet diesen ebenfalls an den Bereitstellungsserver.

Die Aktivierung dieser Einstellung beeinflusst folgende CA IdentityMinder-Funktionen:

- **Registerkarte "Bereitstellungsrollen" in den Benutzeraufgaben**

  Wenn ein Administrator über die Registerkarte "Bereitstellungsrollen" einer Bereitstellungsrolle einen Benutzer hinzufügt oder davon entfernt, kumuliert CA IdentityMinder diese Aktionen zu einem einzelnen Ereignis.

- **Identitätsrichtlinien**

  Alle im Zusammenhang mit der Bereitstellungsrollen-Mitgliedschaft stehenden Ereignisse (AssignProvisioningRoleEvent oder RevokeProvisioningRoleEvent), die als Ergebnis einer Identitätsrichtlinienauswertung generiert werden, werden zu einem einzelnen Ereignis vom Typ "AccumulatedProvisioningRolesEvent" kumuliert. CA IdentityMinder führt dieses Ereignis wie jedes andere sekundäre Ereignis aus. Beispiel: Ein Identitätsrichtliniensatz besteht aus zwei Identitätsrichtlinien: Richtlinie A entfernt die Mitgliedschaft in Bereitstellungsrolle A und Richtlinie B macht Benutzer zu Mitgliedern von Bereitstellungsrolle B. Falls CA IdentityMinder feststellt, dass ein Benutzer der Richtlinie A nicht mehr genügt, dafür jetzt aber Richtlinie B erfüllt, wird ein Ereignis "AccumulatedProvisioningRolesEvent" generiert, dass zwei Aktionen enthält (eine Aktion zum Entfernen und eine Aktion zum Hinzufügen). Als Erstes wird die Aktion für das Hinzufügen und im Anschluss daran die Aktion für das Entfernen ausgeführt.

- **Gesendete Aufgaben anzeigen**

  Wenn Sie sich über den Status des Ereignisses "AccumulatedProvisioningRolesEvent" und den der einzelnen Aktionen informieren möchten, verwenden Sie die Aufgabe "Gesendete Aufgaben anzeigen", mit der Ereignisdetails angezeigt werden können.

  Falls eine der einzelnen Aktionen fehlschlägt, lautet sowohl der Status des Ereignisses als auch der der Aufgabe "Fehlgeschlagen".

- **Workflow**

  Sie können einem Ereignis vom Typ "AccumulatedProvisioningRolesEvent" einen Workflow-Prozess zuordnen. In diesem Fall kann ein Genehmiger das gesamte Ereignis bestätigen oder ablehnen, und damit jedes der einzelnen Ereignisse bestätigen oder ablehnen.

  Soll auch für einzelne Ereignisse innerhalb des AccumulatedProvisioningRolesEvent-Ereignisses Workflow-Kontrolle möglich sein, ist zusätzlicher Konfigurationsaufwand erforderlich.

- **Überprüfung**

  CA IdentityMinder überprüft Informationen zum AccumulatedProvisioningRolesEvent und zu jedem einzelnen Ereignis.

Kumulation der Ereignisse zur Bereitstellungsrollen-Mitgliedschaft ermöglichen

CA IdentityMinder bietet in der Managementkonsole eine Konfigurationseinstellung an, die es ermöglicht, alle Aktionen zum Hinzufügen und Entfernen, die zu einem Ereignis im Zusammenhang mit der Bereitstellungsrollen-Mitgliedschaft gehören, zu einem einzelnen Vorgang zusammenzufassen. Nach der Kombination der Aktionen verarbeitet CA IdentityMinder zunächst die Aktionen zum Hinzufügen als einen einzelnen Vorgang, bevor die Aktionen zum Entfernen verarbeitet werden.

Diese Einstellung ermöglicht die Sequenzierung von Ereignissen, die für einige Endpunkttypen erforderlich ist.

Hinweis: Diese Funktion ist standardmäßig deaktiviert.

So ermöglichen Sie die Kumulation der Ereignisse zur Bereitstellungsrollen-Mitgliedschaft

1. Wechseln Sie zur Managementkonsole von Identity Manager.
2. Klicken Sie auf "Umgebungen".
3. Wählen Sie die Umgebung aus, die Sie konfigurieren möchten.
4. Öffnen Sie "Erweiterte Einstellungen", "Bereitstellung".
5. Wählen Sie das Kontrollkästchen "Enable Accumulation of Provisioning Role Membership Events" (Kumulierung von Ereignissen zur Bereitstellungsrollen-Mitgliedschaft) aus.
6. Starten Sie den Anwendungsserver neu.

Aktivieren von geschachtelten Rollen in einer Umgebung

Sie können eine Bereitstellungsrolle in eine andere Bereitstellungsrolle einschließen. Die eingeschlossene Rolle wird geschachtelte Rolle genannt.

Zum Beispiel könnten Sie eine Mitarbeiter-Bereitstellungsrolle erstellen. Die Mitarbeiter-Rolle würde von allen Mitarbeitern benötigte Konten wie E-Mail-Konten angeben. Sie nehmen die Mitarbeiter-Rolle in abteilungsspezifische Bereitstellungsrollen auf, wie beispielsweise eine Finanz-Rolle und eine Verkaufs-Rolle. Die Abteilungs-Bereitstellungsrollen würden nur auf diese Abteilung bezogene Konten angeben. Diese Kombination von Rollen stellt die richtigen Konten für jeden Benutzer bereit.

So aktivieren Sie geschachtelte Rollen in einer Umgebung

1. Wählen Sie in der Management-Konsole die Umgebung aus.
2. Klicken Sie auf "Rolle" und "Aufgabeneinstellungen", "Importieren".
3. Wählen Sie "Support für geschachtelte Bereitstellungsrollen" aus.

4. Klicken Sie auf "Fertig stellen".
5. Starten Sie die Umgebung neu.

Aufnehmen einer Rolle in eine Bereitstellungsrolle

So schließen Sie eine Rolle in eine Bereitstellungsrolle ein:

1. Klicken Sie auf "Rollen und Aufgaben", "Bereitstellungsrollen", "Bereitstellungsrolle ändern".
2. Stellen Sie die Bereitstellungsrollen-Registerkarte, indem Sie auf "Rolle hinzufügen" klicken und eine Bereitstellungsrolle auswählen.

   Aus Leistungsgründen empfehlen wir, die Rollenschachtelung auf drei Ebenen zu beschränken. Beispielsweise schließen Sie in die aktuelle Bereitstellungsrolle (die Rolle der ersten Ebene) eine andere Rolle (die Rolle der zweiten Ebene) ein, die eine Drittebenen-Rolle enthalten kann. Wir empfehlen, dass die Drittebenen-Rolle keine Rolle enthält.
3. Schließen Sie die Eigentümerrichtlinie durch das Ändern der Eigentümerregel ab.

   Der Bereich muss gleich oder weiter als der Bereich für die Rolle sein, die Sie hinzufügten.
4. Klicken Sie auf "Senden".

Attribute in Kontovorlagen

Die Attribute in Kontovorlagen legen fest, wie Attribute in einem Konto definiert werden.

Funktions- und anfängliche Attribute

Kontovorlagen enthalten zwei Arten von Attributen:

- *Funktionsattribute* stehen für Kontoinformationen wie Speichergröße, Menge, Häufigkeitsbeschränkungen oder Gruppenmitgliedschaften. Der Bereitstellungs-Manager stellt die Funktionsattribute in allen Kontovorlagen-Bildschirmen in Fettschrift dar, damit sie leicht erkennbar sind.
- *Anfängliche Attribute* stehen für alle Informationen, die anfänglich für ein Konto festgelegt wurden, beispielsweise Kontoname, Kennwort und Kontostatus, sowie für persönliche Daten wie Name, Adresse und Telefonnummern.

Konten werden als mit ihren Kontovorlagen synchronisiert betrachtet, wenn alle Funktionsattribute synchronisiert sind. Diese Attribute unterscheiden sich je nach Endpunkttyp, beispielsweise hinsichtlich Gruppenmitgliedschaften, Berechtigungen, Kontingenten oder Anmelde-Einschränkungen. Sie steuern die Möglichkeiten, die der Benutzer hat, wenn er sich bei dem jeweiligen Konto anmeldet.

Bei der Synchronisierung werden keine anderen Kontoattribute aktualisiert. Sie werden aus den Kontovorlagen während der Erstellung von Konten initialisiert, und sie können außerdem während der Durchführung von Propagierungsfunktionen aktualisiert werden. Der Bereitstellungsserver bietet zwei Propagierungsfunktionen (die unmittelbare Aktualisierung von Konten bei einer Änderung der Kontovorlage und die Aktualisierung von Konten bei einer Änderung der globalen Benutzerattribute).

Funktionsattribute und anfängliche Attribute bestimmen

Um herauszufinden, welche Attribute als Funktionen und welche als anfänglich definiert sind, müssen Sie die eTACapability.txt-Datei generieren. Geben Sie den folgenden Befehl in einer Windows-Eingabeaufforderung ein:

```
PS_HOME\dumpptt.exe -c > eTACapability.txt
```

PS_Home

Gibt C:\Program Files\CA\Identity Manager\Provisioning Server\bin an

Eine Dateiversion wird für alle installierten Connectors generiert.

Regelzeichenfolgen für Attribute

Kontoattribute werden unter Verwendung von Regelzeichenfolgen erzeugt. Hierbei handelt es sich um Variablen, die durch den Wert für das jeweilige Konto ersetzt werden. Regelzeichenfolgen sind nützlich, wenn Sie Attribute erzeugen möchten, die nicht bei allen Konten identisch sind. Bei der Regelauswertung ersetzt CA IdentityMinder die Regelzeichenfolgen in den Kontovorlagen durch Daten, die im globalen Benutzerobjekt festgelegt sind.

Hinweis: Die Regelauswertung findet nicht für Konten statt, die im Rahmen einer Durchsuchung erstellt wurden, und ebensowenig für Konten, die ohne Bereitstellungsrollen erstellt wurden.

Da Kontonamen eindeutig sein müssen, sollten Sie eine %AC%-Regelzeichenfolge in das Kontonamen-Feld einer Kontovorlage eingeben. Wenn CA IdentityMinder ein Konto auf der Grundlage dieser Kontovorlage erstellt, verwendet er den Kontonamen des Benutzers.

In der folgenden Tabelle sind die Regelzeichenfolgen für CA IdentityMinder aufgeführt:

Regelzeichenfolge	Beschreibung
%AC%	Kontoname
%D%	Das aktuelle Datum im Format *tt/mm/jjjj* (beim Datum handelt es sich um einen berechneten Wert, der unabhängig von den Daten des globalen Benutzers ist*).* Diese Regelzeichenfolge entspricht einer der folgenden: %$$DATE()% %$$DATE%
%EXCHAB%	Postfach vor Exchange-Adressbuch verbergen
%EXCHS%	Name des Postfach-Basisservers
%EXCMS%	Name des Postfachspeichers
%GENUID%	Numerische UNIX/POSIX-Benutzerkennung. Diese Regelvariable entspricht %UID%, sofern der UID-Wert für den globalen Benutzer festgelegt ist. Wenn dem globalen Benutzer jedoch kein UID-Wert zugewiesen wurde und die UID-Erzeugung aktiviert ist (Global Properties on System Task [Globale Eigenschaften in der Systemaufgabe]), wird der nächste verfügbare UID-Wert zugeordnet, dem globalen Benutzer zugewiesen und als Wert für diese Regelvariable verwendet.
%P%	Kennwort
%U%	Name des globalen Benutzers

Regelzeichenfolge	Beschreibung
%UA%	Vollständige Adresse (wird aus Straße, Stadt, Bundesland/Kanton und Postleitzahl erzeugt)
%UB%	Gebäude
%UC%	Stadt
%UCOMP%	Name der Firma
%UCOUNTRY%	Land
%UCU*xx*% oder %UCU*xxx*%	Benutzerdefiniertes Feld (*xx* oder *xxx*, steht für die zwei- oder dreistellige Feldkennung, die auf der Registerkarte "Custom User Fields (Benutzerdefinierte Benutzerfelder)" in der "System Task (Systemaufgabe)" angegeben ist)
%UD%	Beschreibung
%UDEPT%	Abteilung
%UE%	E-Mail-Adresse
%UEP%	Primäre E-Mail-Adresse
%UES%	Sekundäre E-Mail-Adressen
%UF%	Vorname
%UFAX%	Faxnummer
%UHP%	Startseite
%UI%	Initialen
%UID%	Numerische UNIX/POSIX-Benutzerkennung
%UL%	Nachname
%ULOC%	Verzeichnis
%UMI%	Initialen des zweiten Vornamens
%UMN%	Zweiter Vorname
%UMP%	Mobiltelefonnummer
%UN%	Vollständiger Name
%UO%	Büroname
%UP%	Telefonnummer
%UPAGE%	Pagernummer
%UPC%	Postleitzahl
%UPE%	Telefondurchwahl

Regelzeichenfolge	Beschreibung
%US%	Bundesland/Kanton
%USA%	Postadresse
%UT%	Berufsbezeichnung
%XD%	Erzeugt den aktuellen Zeitstempel im XML-dateTimeValue-Format, einer Zeichenfolge mit fester Länge. Bei einem dateValue- oder timeValue-Attribut können Sie einen Ausdruck für eine untergeordnete Zeichenfolge vom Typ (:offset,length) schreiben, um das Datum oder die Uhrzeit aus dateTimeValue zu extrahieren. So können Sie beispielsweise aus %XD:1,10% den Wert JJJJ-MM-TT und aus %XD:12,8% den Wert HH:MM:SS extrahieren.

Werte für Attribute

Wenn Sie einen spezifischen, konstanten Wert für ein Kontoattribut verwenden möchten, geben Sie diesen Wert im Kontovorlagen-Feld und nicht in Form einer Regelzeichenfolge ein. Auf diese Weise können Sie beispielsweise Werte zum Festlegen von Häufigkeitsbeschränkungen oder der Menge eingeben.

Falls es der konstante Attributwert mehr als ein Prozentzeichen enthalten muss, geben Sie jedes Mal zwei Prozentzeichen (%%) ein. CA IdentityMinder übersetzt diese beim Erzeugen des Kontoattribut-Werts in ein einzelnes Prozentzeichen (%). Wenn der Kontovorlagen-Wert nur ein einzelnes Prozentzeichen enthält, gibt CA IdentityMinder keinen Fehler aus. Entsprechend der Regel muss der Wert "25%" als "25%%" eingegeben werden. Die Schreibweise "25%" wird jedoch als Sonderfall akzeptiert.

Erweiterte Regelausdrücke

Um eine flexiblere Lösung als eine einfache Ersetzung des globalen Benutzerattributs bereitzustellen, können Sie erweiterte Regelausdrücke eingeben, einschließlich des Folgenden:

- Untergeordnete Zeichenfolgen mit Offset und Länge
- Kombinationen aus Regelzeichenfolgen und Werten
- Regelausdrücke, um mehrere Werte für mehrwertige Kontoattribute festzulegen
- Regelvariablen für andere globale Benutzerattribute
- Aufruf integrierter Funktionen
- Aufruf von Program Exit-Funktionen, die vom Kunden geschrieben wurden

Verschmelzen von Regelzeichenfolgen und Werten

Sie können Regelzeichenfolgen und Konstantenwerte zu einem Kontovorlagen-Attributwert verschmelzen. Wenn es z. B. keine %UI%-Regelzeichenfolge gibt, können Sie dieselbe Wirkung erzielen, indem Sie mehrere Regelausdrücke wie folgt zusammenfügen:

```
%UF:,1%%UMI:,1%%UL:,1%
```

Die Regelzeichenfolge %UA% entspricht dem Folgenden:

```
%USA%, %UC%, %US%, %UPC%
```

Sie können auch eine Regelzeichenfolge mit einem Konstantenwert verschmelzen, um einen Endpunktattributwert für ein UNIX-Stammverzeichnis wie folgt zu erstellen:

```
/u/home/%AC%
```

Untergeordnete Zeichenfolgen für Regeln

Beim Folgenden handelt es sich um die Syntax zum Erstellen eines untergeordneten Zeichenfolgenwerts einer Regelvariablen:

```
%var[:offset,length]%
```

var

Repräsentiert den Namen der vordefinierten Regelvariablen entsprechend der Definition aus der Tabelle weiter oben.

offset

(Optional) Definiert den Anfangs-Offset für den Suffix der untergeordneten Zeichenfolge. Die Ziffer 1 repräsentiert das erste Zeichen.

length

(Optional) Definiert den End-Offset für den Suffix der untergeordneten Zeichenfolge. Ein Wert für die Länge des Platzhalters (*) verweist auf das Ende des Werts.

Wenn Sie z. B. als Kontoattribut die ersten 4 Zeichen des Gebäudeattributs eines globalen Benutzers festlegen, definieren Sie die Variable mit Hilfe der folgenden Zeichenfolge:

```
%UB:1,4%
```

Wenn die Zeichenfolge für das Gebäudeattribut leer ist oder aus weniger als vier Zeichen besteht, hat der resultierende Wert für das Kontoattribut weniger als vier Zeichen.

Regelausdrücke mit mehreren Werten

Die meisten Regelausdrücke haben nur einen Wert. Sie beginnen mit einem Benutzerattributwert (der möglicherweise leer ist) und resultieren in einem Kontoattributwert (der möglicherweise auch leer ist). Manchmal ist es jedoch sinnvoll, einen leeren Benutzerattributwert als 0-Wert anzusehen. Manchmal ist es möglicherweise sinnvoll, mehrere Werte zu generieren, um einen Kontoattributwert mit mehreren Werten zu füllen.

Die folgende Regelsyntax lässt die Arbeit mit Null oder mehr Werten zu, die ein Benutzerattribut enthalten kann:

%*var*%

Der optionale Platzhalter für mehrwertige Flags (*) direkt nach dem ersten Prozentzeichen % eines Regelausdrucks gibt an, dass das Ergebnis dieses Regelausdrucks aus 0, 1 oder mehr als 1 Wert bestehen sollte, je nachdem wie viele Werte das referenzierte Benutzerattribut enthält.

Die meisten Benutzerattributwerte haben einen Wert, d. h. sie können nur 0 oder 1 Werte enthalten. Bei den benutzerdefinierten Attributen (CustomField01 bis CustomField99) handelt es sich hingegen um mehrwertige Attribute, d. h. eine Regelvariable, die diese Attribute referenziert, kann 0, 1 oder mehr als 1 Wert enthalten.

Wenn ein Benutzerattribut mehr als einen 1 Wert hat, Sie jedoch das Sternchen (*) im Regelausdruck auslassen, entspricht das Ergebnis der Regelauswertung dem des ersten Werts. In den meisten Fällen sind Attributwerte offiziell nicht geordnet, d. h. es ist nicht vorhersehbar, welchen Wert CA IdentityMinder als ersten Wert einstuft.

Wenn ein Benutzerattribut mehr als einen Wert enthält und * im Regelausdruck enthalten ist, werden mehrere Werte für das Kontoattribut generiert. Sie sollten einen solchen mehrwertigen Regelausdruck nicht in einer Kontovorlage definieren, wenn das Kontoattribut, das aus dem Attribut dieser Kontovorlage festgelegt wird, selbst nicht mehrwertig ist.

Sie können ein erweitertes Kontoattribut im ADS-Endpunkttyp als mehrwertig definieren und mit Hilfe dieser Syntax für mehrwertige Regelausdrücke das Attribut festlegen. Stellen Sie sich z. B. eine Umgebung vor, die ein erweitertes ADS-Kontoattribut mit der Bezeichnung "Patente" definiert, und das dritte benutzerdefinierte Benutzerattribut trägt auch die Bezeichnung "Patente".

Eine ADS-Kontovorlage würde für das Attribut "Patente" die Regelzeichenfolge %*UCU03% definieren. Anschließend könnten Sie das benutzerdefinierte Attribut "Patente" ändern, indem Sie einen oder mehre Werte hinzufügen. Wenn Sie nun diese Änderungen auf den Benutzer anwenden, aktivieren Sie die Option zur Aktualisierung der Konten des Benutzers. Daraufhin wird die Kontovorlage des Kontos überprüft und die Regelvariable %*UCU03% gefunden. Die Anwendung weiß dadurch, dass alle Patente des Benutzers auf das Kontoattribut für Patente kopiert werden sollen.

Auf dieselbe Weise werden beim Erstellen von Konten Regelzeichenfolgen ausgewertet. Wenn darüber hinaus während der Änderung einer Kontovorlage die Regelzeichenfolge geändert wurde, können Sie wahlweise die Regel für alle Konten neu berechnen, denen die Kontovorlage zugeordnet ist.

Die Syntax %*var*% ist auch für Variablen *var* aussagekräftig, die sich auf einwertige Benutzerattribute beziehen. Das trifft nur zu, wenn Konkatenierung verwendet wird und die referenzierten Attribute für Benutzer nicht festgelegt wurden.

Der optionale mehrwertige Platzhalter für Flags (*) gibt an, dass die Regel mit einer %*var*%-Regelvariablen bei der Auswertung keine Werte ergibt, wenn das Benutzerattribut keine Werte enthält. Das unterscheidet sich vom einwertigen Regelausdruck %*var*%, der bei der Auswertung immer einen einzelnen Wert ergibt, selbst wenn es sich dabei um eine leere Zeichenfolge handelt.

Um diesen Unterschied zu verstehen, betrachten Sie die folgenden Regelzeichenfolgen:

```
(310)%UP%
 (310)%*UP%
```

Beide Regelzeichenfolgen hängen anscheinend die Vorwahl 310 an die Telefonnummer. Sie unterscheiden sich jedoch, denn wenn ein Benutzer keinen Wert für die Telefonnummer hat, wird der Kontowert der ersten Regel als (310) ausgewertet. Die zweite Regelzeichenfolge generiert keinen Wert, d. h. das Kontoattribut bleibt nicht festgelegt.

Auf der anderen Seite, bedenken Sie die folgenden Regelzeichenfolgen, die anscheinend die Durchwahlnummer an die Telefonnummer anhängen:

```
%UP% %UPE%
%UP% %*UPE%
```

Wenn jeder eine Telefonnummer hat, aber einige keine Durchwahlnummern, dann generiert die erste Regelzeichenfolge einen Wert, der die Telefonnummer für jeden Benutzer ohne Durchwahlnummer enthält. Die zweite Regelzeichenfolge generiert keine Werte. Verwenden Sie in diesem Fall die erste Regel mit %UPE%.

Explizite Regeln für globale Benutzerattribute

Jeder Benutzer verfügt über viele weitere Attribute, die in der vorherigen Regeltabelle aufgeführt sind. Wahrscheinlich wird es nicht erforderlich sein, dass Sie Regelausdrücke erstellen, die diese anderen Attribute referenzieren. Sollte es jedoch erforderlich sein, können Sie die folgende Syntax verwenden, um eine Referenz auf ein bestimmtes Benutzerattribut zu erstellen:

```
%#ldap-attribute%
```

Wenn Sie z. B. den Feldwert von "Deaktiviert" des Benutzers ermitteln möchten, bestimmen Sie den entsprechenden LDAP-Attributnamen für dieses Feld (d. h. eTSuspended), und Sie erstellen den Regelausdruck, der als 0 oder 1 ausgewertet wird, wie eTSuspended:

```
%#eTSuspended%
```

In einem weiteren Beispiel können Sie die dem Benutzer zugewiesenen Bereitstellungsrollen mit dem folgenden Regelausdruck abrufen:

```
%*#eTRoleDN%
```

Diese Bereitstellungsrollen sind vollständige definierte LDAP-Namenswerte. Vielleicht wären die Werte in Verbindung mit der integrierten RDNVALUE-Funktion (weitere Informationen hierzu finden Sie in der nachfolgenden Tabelle) etwas nützlicher. Beachten Sie das Sternchen (*) als Platzhalter für mehrere Werte, um alle Bereitstellungsrollen als unterschiedliche Werte abzurufen, die dem Benutzer zugewiesen sind.

Die Syntax für untergeordnete Zeichenfolgen gilt auch für diese Regelausdrücke, d. h. Sie könnten %#eTTelephone:6,*% verwenden, um dasselbe auszudrücken wie %UP:6,*. Mit beiden Anweisungen wird CA IdentityMinder aufgefordert, die ersten fünf Zeichen des Feldwerts für das Telefon des Benutzers zu entfernen.

Integrierte Regelfunktionen

Sie können integrierte Regelfunktionen in Ihren Regelausdrücken verwenden, um verschiedene Transformationen auf den Werten durchzuführen. Das allgemeine Format für den Aufruf integrierter Regelfunktionen ist

```
%[*]$$function(arg[,…])[:Offset,Länge]%
```

wobei das Sternchen (*) als Platzhalter für mehrere Werte und die Spezifikationen für die untergeordneten Zeichenfolgen "Offset" und "Länge" auch in diesem Fall optional sind.

Beim Folgenden handelt es sich um anerkannte integrierte Funktionen:

Integrierte Regelfunktion	Beschreibung
ALLOF	Führt alle Parameter zu einem mehrwertigen Attribut zusammen. Die Reihenfolge wird beibehalten und doppelte Werte werden entfernt. Wenn z. B. für Benutzerattribute das Folgende festgelegt wurde: eTCustomField01: { A, B } eTCustomField02: { A, C } Dann wird die Regel: %*ALLOF(%*UCU01%,%*UCU02%)% in drei Werten { A, B, C } ausgewertet.
DATE	Wertet das aktuelle Datum im Format *tt/mm/jjjj* aus. Der Regelausdruck %D% entspricht einem der Folgenden: %$$DATE()% %$$DATE%
FIRSTOF	Gibt den ersten Wert eines beliebigen Parameters zurück. Wird verwendet, um einen Standardwert einzufügen, wenn ein Attribut nicht festgelegt wurde: %$$FIRSTOF(%UCU01%,'unbekannt')% %$$FIRSTOF(%LN%,%UCU01%,%U%)% Wenn keiner der Werte festgelegt wurde, enthält das Ergebnis keine Werte. Um eine Zeichenfolge in Form einer Konstanten in ein Argument einzugeben, setzen Sie sie in einzelne Anführungszeichen.
INDEX	Gibt einen Wert eines mehrwertigen Attributs zurück. Index 1 ist der erste Wert. Wenn der Index größer als die Anzahl der Werte ist, besteht das Ergebnis aus einer leeren Zeichenfolge, d. h. einem nicht festgelegten Wert. Die folgenden Regeln entsprechen dem Folgenden: %$$INDEX(%*UCU01%,1)% %$$FIRSTOF(%*UCU01%)%

Integrierte Regelfunktion	Beschreibung
NOTEMPTY	Gibt den einzigen Wert eines einzelnen Arguments zurück, meldet jedoch einen Fehler, wenn dieser Attributwert nicht festgelegt ist. Beispiel 1: Die Erstellung des Kontos wird mit einem Fehler beendet oder aktualisiert, wenn der Benutzer nicht über ein zugewiesenes UID-Attribut verfügt: %$$NOTEMPTY(%UID%)% Beispiel 2: Verwendet den Vornamen, es sei denn, dieser wurde nicht festgelegt. In einem solchen Fall wird der Nachname verwendet. Wenn keiner von beiden festgelegt wird, wird die Erstellung des Kontos mit einem Fehler beendet oder aktualisiert. %$$NOTEMPTY(%$$FIRSTOF(%UF%, %UL%)%)%
PRIMARYEMAIL	Gibt die primäre E-Mail-Adresse zurück, die aus den unterschiedlichen E-Mail-Adressen extrahiert wurde. Der Ausdruck %UE% entspricht dem Folgenden: %$$PRIMARYEMAIL(%UEP%)%
RDNVALUE	Behandelt den Attributwert als einen definierten LDAP-Namen und extrahiert den allgemeinen Namen des Objekts aus diesem DN: %*$$RDNVALUE(%#eTRoleDN%)% Gibt die allgemeinen Namen aller zugewiesenen Bereitstellungsrollen zurück. Wenn der Benutzer zwei Bereitstellungsrollen mit demselben allgemeinen Namen angehört, wird dieser Rollenname nur einmal aufgeführt.
TOLOWER	Wandelt Text in Großbuchstaben in Kleinbuchstaben um: %$$TOLOWER(%AC%)%
TOUPPER	Wandelt Text in Kleinbuchstaben in Großbuchstaben um: %$$TOUPPER(%U%)%

Integrierte Regelfunktion	Beschreibung
TRIM	Entfernt führende und nachgestellte Leerzeichen von einem Attributwert. So erstellt z. B. "%UF %UL%" allgemein einen Wert, bei dem Vor- und Nachname durch ein Leerzeichen getrennt sind. Wenn das Attribut für den Vornamen des Benutzers jedoch eine leere Zeichenfolge ist, würde diese Regel jedoch einen Wert erzeugen, der mit einem nachgestellten Leerzeichen endet. Wenn Sie jedoch "%$$TRIM(%UF% %UL%)% verwenden, stellen Sie so sicher, dass es keine führenden oder nachgestellten Leerzeichen im Wert des Kontoattributs gibt, selbst wenn der Vorname oder der Nachname nicht festgelegt wurde.

Leistung von Bereitstellungsrollen

Wenn Sie CA IdentityMinder mit einem Bereitstellungsserver verwenden, sollten Sie einige Leistungsverbesserungen für die Bereitstellung in Betracht ziehen.

JIAM-Objekt-Cache

Die Kommunikation zwischen dem Identity Manager und dem Bereitstellungsserver erfolgt mit Hilfe der Java IAM (JIAM) API. Um die Kommunikationsleistung zu verbessern, konfigurieren Sie einen Cache für Objekte, die vom Bereitstellungsserver abgerufen wurden.

Aktivieren Sie den JIAM-Cache

So aktivieren Sie den JIAM-Cache

1. Greifen Sie über die Management-Konsole auf die Umgebungseinstellungen zu. Klicken Sie auf "Erweiterte Einstellungen", "Sonstige".
2. Konfigurieren Sie die benutzerdefinierte Eigenschaft für den JIAM-Cache.
   - **Eigenschaft**–JIAMCache
   - **Wert**–true
3. Klicken Sie auf "Hinzufügen".
4. Klicken Sie auf "Speichern".

   Die benutzerdefinierte Eigenschaft wird gespeichert.

Definieren Sie den TTL-Wert (Time-to-Live = Lebensdauer) für den JIAM-Cache

Im JIAM-Cache werden Informationen für einen bestimmten Zeitraum gespeichert, bevor die Daten ablaufen. Dieser Zeitraum wird als TTL (Time-to-Live) bezeichnet. Sie legen den TTL-Wert (in Sekunden) für den JIAM-Cache fest, um zu definieren, wie lange die Daten im Cache verbleiben.

Um den maximalen Nutzen aus den lokal zwischengespeicherten Daten zu erhalten, führen Sie einen Ausgleich zwischen Leistungsgewinn und Aktualität der Daten durch. Wir empfehlen einen minimalen TTL-Wert von einem Tag mit einem maximalen Wert von 7 Tagen. In der folgenden Tabelle finden Sie Angaben zu TTL-Werten, die verwendet werden sollten:

Gewünschte Lebenszeit	TTL-Einstellungen (Sek.)
24 Stunden (1 Tag)	86.400
72 Stunden (3 Tage)	259.200
120 Stunden (5 Tage)	432.000
168 Stunden (7 Tage)	604.800

So definieren Sie den TTL-Wert für den JIAM-Cache

1. Greifen Sie über die Management-Konsole auf die Umgebung zu. Klicken Sie auf "Erweiterte Einstellungen", "Sonstige".
2. Konfigurieren Sie die benutzerdefinierte Eigenschaft für den TTL-Wert des JIAM-Cache.
   - **Eigenschaft**–JIAMCacheTTL
   - **Wert**–Anzahl der Sekunden, die die Daten im JIAM-Cache verbleiben

     Standard: 300
3. Klicken Sie auf "Hinzufügen".
4. Klicken Sie auf "Speichern".

   Die benutzerdefinierte Eigenschaft wird gespeichert.

Sitzungspools

Um die Leistung zu verbessern, kann Identity Manager im Voraus mehrere Sitzungen zuweisen, die aus dem Pool verwendet werden können, wenn eine Kommunikation mit dem Bereitstellungsserver aufgebaut wird.

Weitere Informationen zu Sitzungspools finden Sie in der *Online-Hilfe zur Management-Konsole.*

Provisionierung von Aufgaben für vorhandene Umgebungen

Wenn Sie benutzerdefinierte Rollendefinitionen importieren und die Bereitstellung in einer Umgebung aktivieren möchten, müssen Sie *auch* die Rollendefinitionen "Nur Bereitstellung" in der Management-Konsole importieren. Diese Rollendefinitionen finden Sie im folgenden Ordner:
`iam_im.ear\management_console.war\WEB-INF\Template\environment`

Hinweis: Weitere Informationen über das Importieren von Rollendefinitionen finden Sie im *Konfigurationshandbuch*.

Kapitel 10: Verwaltete Services (Basiszugriffsanfragen)

Dieses Kapitel enthält folgende Themen:

Erstellen von Services (siehe Seite 244)
Services für Benutzer verfügbar machen (siehe Seite 255)
Einen Service ändern (siehe Seite 259)
Einen Service löschen (siehe Seite 261)
Erneuern des Zugriffs auf Services (siehe Seite 263)

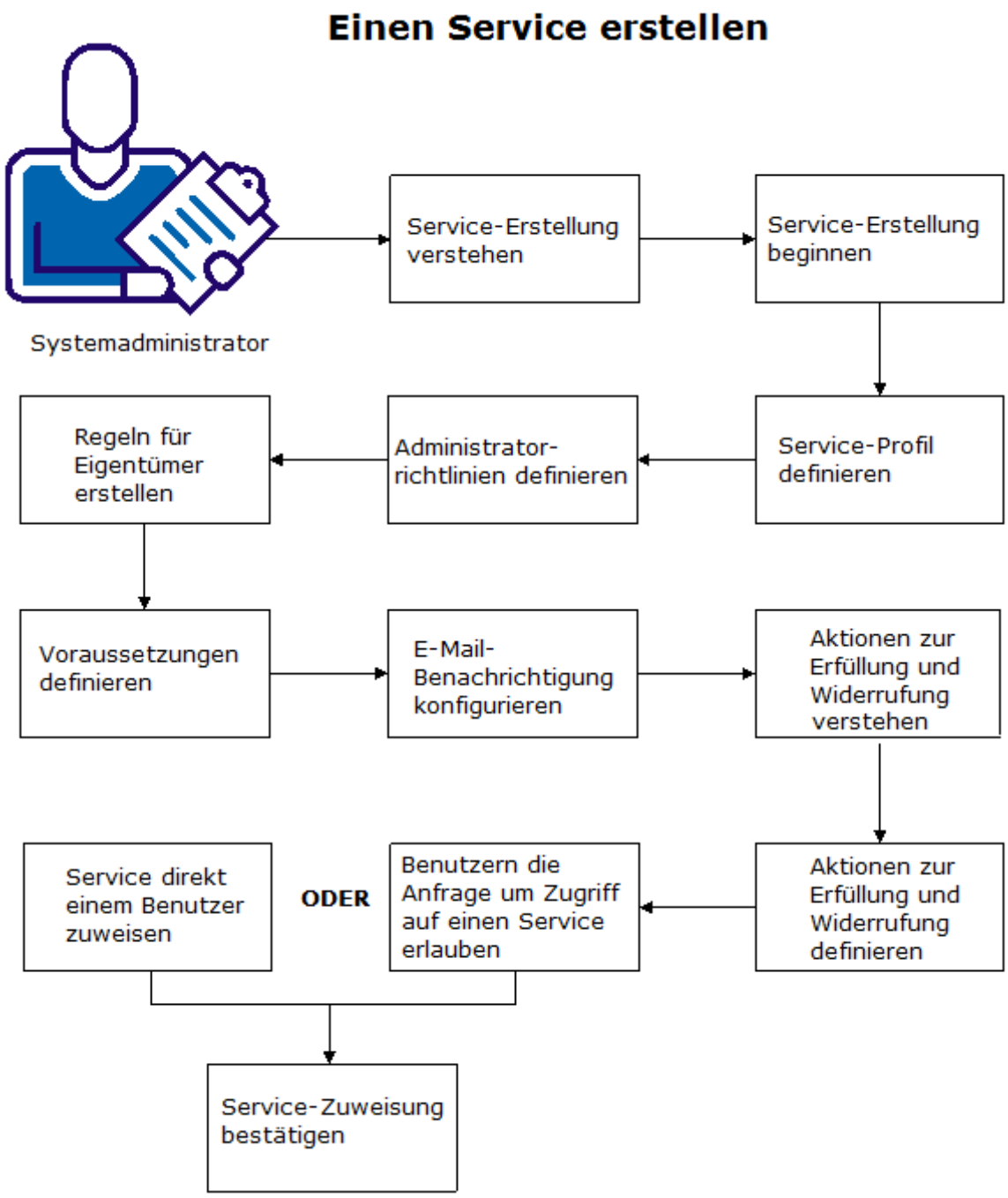
Erstellen von Services

Services vereinfachen die Berechtigungsverwaltung. Ein Dienst bündelt alle Berechtigungen (Aufgaben, Rollen, Gruppen und Attribute), die ein Benutzer für eine bestimmte Unternehmensrolle benötigt. Services sind für den Benutzer über Zugriffsanfrage-Aufgaben in der CA CloudMinder Benutzerkonsole verfügbar. Zugriffsanfrage-Aufgaben ermöglichen einem Benutzer oder Administrator, einen Service anzufordern, zuzuweisen, zu widerrufen und zu erneuern.

Dienste ermöglichen einem Administrator, Benutzerberechtigungen in einem einzigen Paket zu kombinieren, die dann als ein Set verwaltet werden. Zum Beispiel benötigen alle neuen Vertriebsmitarbeiter Zugriff auf einen definierten Satz von Aufgaben und auf Konten von bestimmten Endpunktsystemen. Sie benötigen auch bestimmte Informationen, die zu ihren Benutzerkontoprofilen hinzugefügt wurden. Ein Systemadministrator erstellt einen Service namens Vertriebsverwaltung, der alle erforderlichen Aufgaben, Rollen, Gruppen und Profilattributinformation für einen neuen Vertriebsmitarbeiter enthält. Wenn ein Administrator den Service "Vertriebsverwaltung" einem Benutzer zuweist, erhält dieser Benutzer die gesamte Gruppe an Rollen, Aufgaben, Gruppen und Kontoattributen, die vom Service definiert werden.

Eine weitere Möglichkeit, wie Benutzer auf Services zugreifen können, ist mit einer eigenen Zugriffsanfrage. In der Benutzerkonsole hat jeder Benutzer eine Liste von Services, die für seine Anfrage verfügbar sind. Diese Liste wird mit Services gefüllt, die von einem Administrator mit den entsprechenden Berechtigungen als "Selbstabonnierend" markiert wurden, normalerweise während der Service-Erstellung. Über die Liste der verfügbaren Services können Benutzer den Zugriff auf die benötigten Services anfordern. Wenn der Benutzer Zugriff auf einen Service anfordert, wird die Anfrage automatisch erfüllt, und die zugeordneten Berechtigungen werden dem Benutzer sofort zugewiesen. Ein Administrator mit den entsprechenden Berechtigungen kann die Service-Abwicklung auch so konfigurieren, dass eine Workflow-Genehmigung erforderlich ist oder E-Mail-Benachrichtigungen generiert werden.

Das folgende Diagramm zeigt alle wichtigen Informationen und die Schritte zum Ausführen oder Erstellen eines Service.


Einen Service erstellen
Systemadministrator
Service-Erstellung verstehen
Service-Erstellung beginnen
Service-Profil definieren
Administrator-richtlinien definieren
Regeln für Eigentümer erstellen
Voraussetzungen definieren
E-Mail-Benachrichtigung konfigurieren
Aktionen zur Erfüllung und Widerrufung verstehen
Aktionen zur Erfüllung und Widerrufung definieren
Benutzern die Anfrage um Zugriff auf einen Service erlauben
ODER
Service direkt einem Benutzer zuweisen
Service-Zuweisung bestätigen

In den folgenden Themen wird erklärt, wie Sie einen Service erstellen und ihn Benutzern zur Verfügung stellen:

1. Wissenswertes über die Service-Erstellung (siehe Seite 246)
2. Einführung in die Service-Erstellung (siehe Seite 247)
3. Definieren des Service-Profils (siehe Seite 247)
4. Definieren der Admin-Richtlinien für den Service (siehe Seite 249)
5. Definieren der Eigentümerregeln für den Service (siehe Seite 250)
6. Definieren der Voraussetzungen für den Service (siehe Seite 250)
7. Konfigurieren der E-Mail-Benachrichtigung für die Service-Erneuerung (siehe Seite 251)
8. Wissenswertes über Abwicklungs- und Annulierungsaktionen (siehe Seite 252)
9. Definieren der Abwicklungs- und Annulierungsaktionen für den Service (siehe Seite 252)
10. Erlauben Sie Benutzern, Zugriff auf Services anzufordern.

    Wenn der Benutzer in der Benutzerkonsole auf "Mein Zugriff" und dann auf "Zugriff anfordern und anzeigen" klickt, wird eine Liste der für seine Anfrage verfügbaren Services aufgelistet. Die Services, die in dieser Liste angezeigt werden, wurden von einem Administrator mit den entsprechenden Berechtigungen als "Selbstabonnierend" markiert, normalerweise während der Service-Erstellung.
11. Weisen Sie einen Service direkt einem Benutzer zu (siehe Seite 89).
12. Bestätigen Sie die Service-Zuweisung (siehe Seite 255).

Wissenswertes über die Service-Erstellung

Bevor Sie einen Service erstellen, beachten Sie die vorausgesetzten Informationen und Berechtigungen, die erforderlich sind, um den Service zu erstellen und abzuwickeln.

Beantworten Sie folgende Fragen:

1. Welcher Geschäftsanforderung entspricht dieser Service? Zum Beispiel können Sie einen Service erstellen, der allen neuen Mitarbeitern ein Konto auf Salesforce.com zur Verfügung stellt.
2. Benötigen Mitglieder eines Service gewisse Admin-Rollen? Falls ja, erstellen oder identifizieren Sie diese Admin-Rollen.
3. Müssen Mitglieder des Service Zugriff auf einen oder mehrere Endpunkte erhalten? Falls ja, erstellen oder identifizieren Sie diese Endpunkte.
4. Wenn Service-Mitglieder auf Endpunkte zugreifen, erstellen oder identifizieren Sie die zugeordneten Bereitstellungsrollen und Kontovorlagen.

5. Müssen Mitglieder des Service Mitglieder bestimmter Gruppen sein? Falls ja, erstellen oder identifizieren Sie diese Endpunkte.
6. Müssen bestimmte Benutzerattribute referenziert oder geändert werden, wenn ein Benutzer Mitglied eines Service wird? Beispiel: Wenn ein Benutzer den Salesforce.com-Service empfängt, muss dann bestätigt werden, ob das Abteilungsattribut für diesen Benutzer auf Vertrieb festgelegt wird? Falls ja, erstellen oder identifizieren Sie diese Benutzerattribute.

Sobald Sie diese Voraussetzungen erstellt oder identifiziert haben, können Sie mit der Service-Erstellung (siehe Seite 247) anfangen.

Einführung in die Service-Erstellung

Services werden über die Benutzerkonsole erstellt.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei einem Konto mit Serviceverwaltungsberechtigungen an.

   Dem ersten Benutzer einer Umgebung ist beispielsweise die System-Manager-Rolle zugewiesen, welche die Aufgabe "Service ändern" aufweist.
2. Wählen Sie im Navigationsmenü "Services" aus.
3. Klicken Sie auf "Services verwalten" und "Service erstellen".
4. Definieren des Service-Profils

Definieren des Service-Profils

Auf der Registerkarte "Profil" werden grundlegende Eigenschaften des Service definiert.

Gehen Sie wie folgt vor:

1. Geben Sie einen Namen und ein Tag ein. Ein Tag ist eine eindeutige Kennung für den Service.

   Hinweis: Tags können nur alphanumerische Zeichen und Unterstriche enthalten und dürfen nicht mit einer Zahl anfangen. Nach dem Erstellen kann ein Tag-Name nicht geändert oder erneut verwendet werden, auch wenn ein Service später gelöscht wird.
2. Wählen Sie die Option "Aktiviert" aus, wenn Sie den Service sofort nach der Erstellung für die Verwendung freigeben möchten.
3. Wählen Sie "Selbstabonnierend" aus, wenn Sie möchten, dass dieser Service in der Liste der Services angezeigt wird, die Benutzern zur Anfrage zur Verfügung stehen. Wenn "Selbstabonnierend" aktiviert ist, können Benutzer Zugriff auf diesen Service über die Benutzerkonsole anfordern.

4. (Optional) Fügen Sie eine oder mehrere Kategorien hinzu. Geben Sie einen Kategorienamen ein und klicken Sie auf den Pfeil nach oben, um sie zum Service hinzuzufügen.

   Kategorien fügen einem Service Zusatzinformationen hinzu. Sie können diese zusätzlichen Informationen verwenden, um die Suche nach Services in Umgebungen zu erleichtern, die eine große Anzahl von Services enthalten.

5. Geben Sie ein Benutzerdatenfenster für Service-Laufzeit an, wenn Sie zusätzliche Benutzerdaten erfassen möchten, sobald ein Benutzer den Service anfordert.

   Verwenden Sie ein Benutzerdatenfenster für Service-Laufzeit, um sicherzustellen, dass alle zum Abwickeln des Service erforderlichen Benutzerdaten im System vorhanden sind. Zum Beispiel ist eine gültige E-Mail-Adresse erforderlich, um einen Service abzuwickeln, der ein Konto in Google Apps erstellt. Wenn eine E-Mail-Adresse für einen Benutzer im CA CloudMinder-Benutzerspeicher nicht vorhanden ist, muss der Benutzer sie angeben, wenn er den Service anfordert.

   a. Klicken Sie auf "Durchsuchen".

      Eine Liste der verfügbaren Profilfenster wird angezeigt. Diese Fenster werden normalerweise verwendet, um Benutzerdaten zu erfassen.

   b. Wählen Sie ein Profilfenster aus, das die Benutzerdaten enthält, die Sie erfassen wollen. Wählen Sie eine der folgenden Optionen aus:

      - Klicken Sie auf "Auswählen", um alle enthaltenen Benutzerdaten in diesem Fenster zu erfassen.

      ODER

      - Klicken Sie auf "Kopieren", um die Benutzerdaten anzupassen, die Sie erfassen wollen. Geben Sie einen Namen und einen eindeutigen Tag für das neue Fenster an. Fügen Sie Benutzerdatenelemente hinzu, bearbeiten oder entfernen Sie sie, und klicken Sie auf "OK".

      ODER

      - Klicken Sie auf "Bearbeiten", um die in diesem Fenster enthaltenen Benutzerdaten zu ändern. Fügen Sie Benutzerdatenelemente hinzu, bearbeiten oder entfernen Sie sie, und klicken Sie auf "OK".

      Wichtig! Wenn Sie ein Benutzerdatenfenster bearbeiten, werden Ihre Änderungen überall angewendet, wo das Fenster in der Benutzerkonsole verwendet wird. Sie können das Profilfenster stattdessen auch kopieren und anpassen.

   c. Klicken Sie auf "Auswählen".

      Die von Ihnen ausgewählten Benutzerdatenelemente werden zu dem Zeitpunkt erfasst, an dem der Benutzer den Service anfordert.

      Hinweis: Wenn die erforderlichen Daten im System vorhanden sind, wenn ein Benutzer den Service anfordert, werden die Daten im Profilfenster vorab ausgefüllt.

6. Definieren der Admin-Richtlinien für den Service (siehe Seite 249)

Definieren der Admin-Richtlinien für den Service

Auf der Registerkarte "Administratoren" definieren Sie, wer Benutzer als Mitglieder und Administratoren dieses Service hinzufügen oder entfernen kann. Admin-Richtlinien enthalten Admin- und Bereichsregeln und mindestens eine Administratorberechtigung (Mitglieder verwalten oder Administratoren verwalten).

Admin-Regeln bestimmen, wer diesen Service verwalten kann. Bereichsregeln schränken ein, welche Benutzer Administratoren werden können. Zum Beispiel kann eine Admin-Regel allen Mitgliedern der Vertriebsgruppe erlauben, einen Service zu verwalten. Eine Bereichsregel kann dann diese Benutzer auf Vertriebsgruppen-Mitglieder in Berlin beschränken.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administratoren" auf "Hinzufügen".

   Das Fenster "Admin-Richtlinie" wird angezeigt.

2. Definieren Sie eine Admin-Regel, welche Benutzer diesen Service verwalten können. Zum Beispiel können Sie Benutzer angeben, die Mitglieder der Vertriebsgruppe sind oder die das spezielle Jobtitel-Profilattribut für Vertriebs-Manager haben.

   Klicken Sie auf den linken Pfeil, um einen zuvor angegebenen Teil einer Regel zu bearbeiten.

3. Definieren Sie eine Bereichsregel, um einzuschränken, welche Benutzer diesen Service verwalten können. Wenn Sie beispielsweise in der Admin-Regel Benutzer angegeben haben, die Vertriebsgruppen-Mitglieder sind, können Sie anschließend den Bereich dieser Regel auf Benutzer beschränken, deren Stadt Berlin ist.

   Hinweis: Sie können mehrere Admin-Richtlinien mit unterschiedlichen Regeln und unterschiedlichen Berechtigungen für jeden Service hinzufügen.

4. Wenn Sie Administratoren erlauben wollen, Mitglieder für diesen Service hinzuzufügen oder zu entfernen, klicken Sie auf "Kann Mitglieder dieses Service verwalten".

5. Klicken Sie auf "OK".

6. Um eine Richtlinie weiter zu bearbeiten, klicken Sie auf das Symbol "Bearbeiten". Um eine Richtlinie zu entfernen, klicken Sie auf das Minuszeichen.

7. Definieren der Eigentümerregeln für den Service (siehe Seite 250)

Definieren der Eigentümerregeln für den Service

Auf der Registerkarte "Eigentümer" definieren Sie Regeln darüber, wer Eigentümer des Service sein kann. Ein Eigentümer ist ein Benutzer, der den Service ändern kann.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administratoren" auf "Hinzufügen".

   Das Fenster "Eigentümerregel" wird angezeigt.

2. Definieren Sie eine Admin-Regel, welche Benutzer diesen Service verwalten können. Zum Beispiel können Sie Benutzer angeben, die Mitglieder der Vertriebsgruppe sind oder die das spezielle Jobtitel-Profilattribut für Vertriebs-Manager haben.

   Klicken Sie auf den linken Pfeil, um einen zuvor angegebenen Teil einer Regel zu bearbeiten.

3. Klicken Sie auf "OK".

4. Definieren der Voraussetzungen für den Service (siehe Seite 250)

Definieren der Voraussetzungen für den Service

Auf der Registerkarte "Voraussetzungen" definieren Sie Services, die Benutzer haben müssen, bevor sie diesen Service anfordern. Ein Service wird nur in der Liste der verfügbaren Services für einen bestimmten Benutzer angezeigt, wenn dieser Benutzer ein Mitglied von allen erforderlichen Services ist.

Wenn eine Dauer für einen vorausgesetzten Service festgelegt wird, bezieht sich diese Dauer auf den Service, den Sie definieren. Beispielsweise ist Service A eine Voraussetzung für Service B. Service A hat eine Dauer von einer Woche. Service B läuft auch nach einer Woche ab.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Voraussetzungen" auf "Service hinzufügen".

   Ein Suchfenster wird geöffnet.

2. Suchen Sie nach einem Service, den Sie als Voraussetzung für diesen Service bestimmen wollen.

   Um eine Liste aller Services anzuzeigen, für die Sie Administratorrechte haben, klicken Sie auf "Suchen", ohne die Suchkriterien zu ändern.

3. Wählen Sie einen Service aus, und klicken Sie auf "Auswählen".

   Eine aktualisierte Liste von Voraussetzungen für diesen Service wird angezeigt.

Konfigurieren der E-Mail-Benachrichtigung für die Service-Erneuerung

Einige Services laufen nach einer gewissen Frist ab.

Auf der E-Mail-Registerkarte können Sie eine E-Mail-Benachrichtigung konfigurieren, die Servicemitglieder daran erinnert, ihre Mitgliedschaft vor Ablauf zu erneuern. Mitglieder können dann die Aufgabe "Service erneuern" verwenden, um ihren Zugriff zu erneuern.

CA CloudMinder bietet eine standardmäßige E-Mail-Vorlage an, die dynamischen Inhalt einschließt. Dieser Inhalt wird automatisch ausgefüllt, wenn die E-Mail gesendet wird. Dynamischer Inhalt, der in geschweiften Klammern ({ }) im E-Mail-Benachrichtigungs-Editor angezeigt wird, fügt einen bestimmten Benutzernamen, Servicenamen und das Ablaufdatum zur E-Mail hinzu.

Sie können den Inhalt der E-Mail-Benachrichtigung im Editor ändern. Zum Beispiel können Sie den Text oder Betreff anpassen, die Schriftart ändern oder dynamischen Inhalt entfernen.

Beachten Sie die folgenden Elemente beim Konfigurieren von E-Mail-Benachrichtigungen:

- Wenn Sie dynamischen Inhalt in die E-Mail-Benachrichtigung einschließen, ändern Sie nicht den Text zwischen den geschweiften Klammern ({ }).
- Wenn der Service einen erforderlichen Service hat, der abläuft, werden E-Mail-Benachrichtigungen nur für den erforderlichen Service gesendet, auch wenn E-Mail-Benachrichtigungen für beide Services konfiguriert sind.

Gehen Sie wie folgt vor:

1. Aktivieren Sie auf der E-Mail-Registerkarte das Kontrollkästchen "Benachrichtigung der Benutzer per E-Mail bevor ein Service abläuft", um Benachrichtigungen zu aktivieren.
2. (Optional) Passen Sie die E-Mail-Benachrichtigung mithilfe der Steuerelemente im Editor an.

   Der E-Mail-Benachrichtigungs-Editor unterstützt HTML. Sie können dem Text der E-Mail-Benachrichtigung HTML-Inhalt hinzufügen, indem Sie in der Symbolleiste auf die Schaltfläche zum Umschalten des HTML-Quellcodes (<>) klicken.
3. Wissenswertes über Abwicklungs- und Annulierungsaktionen (siehe Seite 252)

Wissenswertes über Abwicklungs- und Annulierungsaktionen

Auf der Registerkarte "Aktionen" definieren Sie die Berechtigungen und Informationen – Aufgaben, Rollen, Gruppen und Attribute – die hinzugefügt, geändert oder entfernt werden sollen, wenn ein Service zugewiesen oder widerrufen wird. Einfach gesagt, Serviceaktionen bestimmen die Aktionen, die ein Service ausführt.

CA CloudMinder verwendet eine Policy Xpress-Richtlinie, um die Umstände zu definieren, unter denen Abwicklungs- und Annulierungsaktionen auftreten. CA CloudMinder hat diese Richtlinie vorkonfiguriert, sodass immer, wenn ein Benutzer einen Service anfordert, die richtigen Bedingungen und Daten vorhanden sind. Der Service wird automatisch abgewickelt oder widerrufen.

Ein Administrator muss die Aktionen definieren, die das System beim Abwickeln oder Annullieren eines Service ausführt. Zum Beispiel kann ein Administrator beim Erstellen eines Service angeben, dass Service-Mitglieder die Admin-Rolle "Vertriebs-Manager", die Salesforce.com-Bereitstellungsrolle und die Vertriebsgruppe erhalten. Außerdem kann der Administrator angeben, dass diese Berechtigungen entfernt werden, wenn der Service widerrufen wird.

Definieren der Abwicklungs- und Annulierungsaktionen für den Service

Auf der Registerkarte "Aktionen" definieren Sie die Berechtigungen und Informationen, die das System hinzufügt, ändert oder entfernt, wenn ein Service einem Benutzer zugewiesen oder von diesem entfernt wird.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte "Aktionen".

   Das Fenster für Abwicklungs- und Annulierungsaktionen wird angezeigt.

2. Klicken Sie auf die Schaltfläche "Abwicklungsaktionen verwalten" oder "Annulierungsaktionen verwalten".

   Das Fenster "Policy Xpress-Richtlinie erstellen" wird angezeigt.

   Die folgenden Felder sind für die Erstellung einer Aktionsregel bereits definiert:

   Name

   Gibt einen Anzeigenamen für die Aktionsregel an. Dieser Name muss eindeutig sein.

   Beschreibung

   Definiert die Bedeutung der Aktionsregel.

   Priorität

   Definiert, welche Aktionsregel ausgeführt wird, falls mehrere Aktionsregeln übereinstimmen. Dieses Feld ist zum Definieren von Standardaktionen hilfreich. Wenn Sie beispielsweise mehrere Regeln haben, jeweils eine für einen Abteilungsnamen, ist es möglich, eine Standardaktion festzulegen, indem Sie eine zusätzliche Regel ohne Bedingungen, aber mit einer niedrigeren Priorität (z. B. 10, wenn alle anderen 5 haben) hinzufügen. Wenn für keine der Abteilungsregeln eine Übereinstimmung gefunden wird, wird die Standardaktion verwendet.

3. Geben Sie unter "Bedingungen der Aktionsregel" Kriterien an, die erfüllt sein müssen.

4. Klicken Sie unter "Hinzufügungsaktion" auf die Schaltfläche "Hinzufügungsaktion bei Übereinstimmung".

   Das Fenster "Hinzufügungsaktion bei Übereinstimmung" wird geöffnet. Definieren Sie in diesem Fenster die Aktionen, die das System bei Übereinstimmung mit der Regel ausführt.

5. Geben Sie einen aussagekräftigen Namen ein, der den Zweck der Aktion definiert.

   Geben Sie zum Beispiel "Admin-Rolle Vertriebs-Manager hinzufügen" ein.

6. Wählen Sie die Kategorie der Aktion aus, die das System ausführen soll.

   Um zum Beispiel eine Rolle hinzuzufügen, wählen Sie die Kategorie "Rollen" aus.

7. Wählen Sie die Kategorie der Aktion aus, die das System ausführen soll.

   Um zum Beispiel eine Admin-Rolle hinzuzufügen oder zu entfernen, wählen Sie den Typ "Admin-Rolle festlegen" aus.

8. Wählen Sie die Funktion aus, die das System ausführen soll.

   Um zum Beispiel eine Admin-Rolle hinzuzufügen, wählen Sie die Funktion "Hinzufügen" aus.

   Hinweis: Wenn Sie eine Funktion auswählen, wird eine Beschreibung dieser Funktion angezeigt. Diese Beschreibung kann Ihnen dabei helfen, zu entscheiden, ob die ausgewählte Funktion zu dem gewünschten Systemverhalten führt.

9. Definieren Sie die jeweilige Aktion, die das System ausführen soll.

   Um zum Beispiel eine Admin-Rolle "Vertriebs-Manager" hinzuzufügen, geben Sie den Rollennamen ein, oder klicken Sie auf die Schaltfläche "Durchsuchen" und wählen Sie "Vertriebs-Manager" aus der Liste der verfügbaren Admin-Rollen aus.

10. Klicken Sie auf "OK".

    Wiederholen Sie diesen Vorgang, bis Sie alle gewünschten Aktionen für diesen Dienst hinzugefügt haben.

11. Klicken Sie auf "OK".

    Das System weist die definierten Abwicklungs- und Annulierungsaktionen mit dem Service zu. Wenn ein Benutzer den Service erhält, werden die zugeordneten Berechtigungen und Informationen hinzugefügt, geändert oder entfernt.

12. Sie können jetzt einen Service einem Benutzer zuweisen (siehe Seite 89).

Weisen Sie einen Service einem Benutzer zu.

Sie können einen Service direkt einem individuellen Benutzer zuweisen. Dieser Benutzer wird ein *Mitglied* des Services.

Gehen Sie wie folgt vor:

1. Wählen Sie im Navigationsmenü "Services" und "Zugriff anfordern und anzeigen".

   Eine Liste von Services, die Sie verwalten können, wird angezeigt.

2. Wählen Sie den Service aus, den Sie einem Benutzer zuweisen möchten, und klicken Sie auf "Auswählen".

   Eine Liste von Benutzern, die dem Service zugewiesen sind, wird angezeigt.

3. Klicken Sie auf "Zugriff anfordern".

4. Suchen Sie nach dem Benutzer, dem Sie den Service zuweisen möchten.

   Um eine Liste aller Benutzer anzuzeigen, für die Sie Administratorrechte haben, klicken Sie auf "Suchen", ohne die Suchkriterien zu ändern.

5. Wählen Sie einen Benutzer aus, und klicken Sie auf "Auswählen".

   Eine aktualisierte Liste von Benutzern, die dem Service zugewiesen sind, wird angezeigt.

6. Klicken Sie auf "Änderungen speichern".

   Der angegebene Service wird für den Benutzer durchgeführt. Der Benutzer erhält alle im Service enthaltenen Anwendungen, Rollen, Gruppen und Attribute.

Servicezuweisung bestätigen

Sobald Sie einem Benutzer einen Service zugewiesen haben, bestätigen Sie, dass alle mit dem Service verknüpften Aufgaben erfolgreich abgeschlossen wurden.

Gehen Sie wie folgt vor:

1. Wählen Sie im Navigationsmenü "Services" und "Verlauf der Service-Zugriffsanfragen anzeigen" aus.

   Ein Suchfenster wird geöffnet.

2. Suchen Sie nach dem Service, den Sie einem Benutzer zugewiesen haben.

   Um eine Liste aller Services anzuzeigen, für die Sie Administratorrechte haben, klicken Sie auf "Suchen", ohne die Suchkriterien zu ändern.

   Eine Liste von Services, die Sie verwalten können, wird angezeigt.

3. Wählen Sie den Service aus, den Sie zugewiesen haben, und klicken Sie auf "Auswählen".

   Ein Verlauf von Aktionen, die mit dem Service verknüpft sind, wird angezeigt.

4. Klicken Sie auf "Letzte Änderung", um die aktuellsten Aktionen zuerst zu sehen.

5. Bestätigen Sie, dass der Service für den entsprechenden Benutzer erfolgreich durchgeführt wurde.

6. Klicken Sie auf "Schließen".

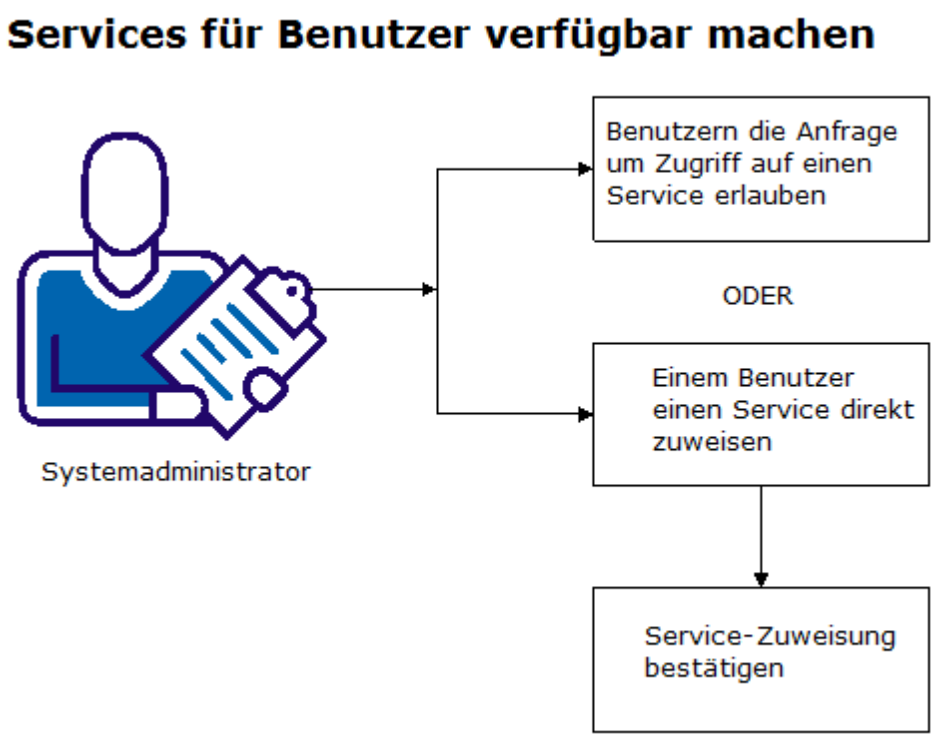
Services für Benutzer verfügbar machen

Services vereinfachen die Berechtigungsverwaltung. Ein Service bündelt alle Berechtigungen, die ein Benutzer für eine bestimmte Geschäftsrolle benötigt. Services sind für den Benutzer über Zugriffsanfrage-Aufgaben in der Benutzerkonsole verfügbar. Zugriffsanfrage-Aufgaben ermöglichen einem Benutzer oder Administrator, einen Service über die Benutzeroberfläche anzufordern, zuzuweisen, zu widerrufen und zu erneuern.

Services erlauben einem Systemadministrator, Benutzeraktivitäten und Informationen (Aufgaben, Rollen, Gruppen und Attribute), die als Gruppe verwaltet werden, in einem einzelnen Paket zu kombinieren. Beispiel: Alle neuen Vertriebsmitarbeiter benötigen Zugriff auf eine definierte Aufgabengruppe, Konten auf speziellen Endpunktsystemen und spezifische Informationen, die ihren Benutzerkontenprofilen hinzugefügt wurden. Ein Systemadministrator erstellt einen Service namens Vertriebsverwaltung, der alle erforderlichen Aufgaben, Rollen, Gruppen und Profilattributinformation für einen neuen Vertriebsmitarbeiter enthält. Wenn ein Administrator den Service "Vertriebsverwaltung" einem Benutzer zuweist, erhält dieser Benutzer die gesamte Gruppe an Rollen, Aufgaben, Gruppen und Kontoattributen, die vom Service definiert werden.

Eine weitere Möglichkeit, wie Benutzer auf Services zugreifen können, ist mit einer eigenen Zugriffsanfrage. In der Benutzerkonsole hat jeder Benutzer eine Liste von Services, die für seine Anfrage verfügbar sind. Diese Liste wird mit Services gefüllt, die von einem Systemadministrator mit den entsprechenden Berechtigungen als "Selbstabonnierend" markiert wurden, normalerweise während der Service-Erstellung. Über die Liste der verfügbaren Services können Benutzer den Zugriff auf die benötigten Services anfordern. Wenn ein Benutzer den Zugriff auf einen Service anfordert, wird die Anforderung automatisch verarbeitet. Die zugeordneten Aufgaben, Rollen, Gruppen und Attribute werden dem Benutzer sofort zugewiesen. Ein CA CloudMinder-Administrator mit den entsprechenden Berechtigungen kann die Service-Abwicklung auch so konfigurieren, dass eine Workflow-Genehmigung erforderlich ist oder E-Mail-Benachrichtigungen generiert werden.

Das folgende Diagramm zeigt die Informationen und Schritte, um Benutzern Services zur Verfügung zu stellen.


Services für Benutzer verfügbar machen
Benutzern die Anfrage um Zugriff auf einen Service erlauben
ODER
Einem Benutzer einen Service direkt zuweisen
Service-Zuweisung bestätigen
Systemadministrator

Sie können Benutzern Services wie folgt zur Verfügung stellen:

1. Erlauben Sie Benutzern, den Zugriff selbst anzufordern.

   Wenn der Benutzer in der CA CloudMinder-Benutzerkonsole auf "Mein Zugriff" und dann auf "Zugriff anfordern und anzeigen" klickt, wird eine Liste der für seine Anfrage verfügbaren Services aufgelistet. Die Services, die in dieser Liste angezeigt werden, wurden von einem CA CloudMinder-Administrator mit den entsprechenden Berechtigungen als "Selbstabonnierend" markiert, normalerweise während der Service-Erstellung.

   Wenn der Benutzer Zugriff anfordert, weist das System den Service dem Benutzer zu. Der Benutzer erhält alle zum Service zugeordneten Anwendungen, Rollen, Gruppen und Attribute. Wenn der Service eine Startrolle für eine Anwendung enthält, werden ein Symbol und ein Link zur Anwendung in der Benutzerkonsolen-Startseite angezeigt.

2. Weisen Sie einen Service direkt einem Benutzer zu (siehe Seite 89).

3. Wenn Sie einen Service direkt einem Benutzer zuweisen, bestätigen Sie die Servicezuweisung (siehe Seite 258).

Weisen Sie einen Service einem Benutzer zu.

Sie können einen Service direkt einem individuellen Benutzer zuweisen. Dieser Benutzer wird ein *Mitglied* des Services.

Gehen Sie wie folgt vor:

1. Wählen Sie im Navigationsmenü "Services" und "Zugriff anfordern und anzeigen".

   Eine Liste von Services, die Sie verwalten können, wird angezeigt.

2. Wählen Sie den Service aus, den Sie einem Benutzer zuweisen möchten, und klicken Sie auf "Auswählen".

   Eine Liste von Benutzern, die dem Service zugewiesen sind, wird angezeigt.

3. Klicken Sie auf "Zugriff anfordern".

4. Suchen Sie nach dem Benutzer, dem Sie den Service zuweisen möchten.

   Um eine Liste aller Benutzer anzuzeigen, für die Sie Administratorrechte haben, klicken Sie auf "Suchen", ohne die Suchkriterien zu ändern.

5. Wählen Sie einen Benutzer aus, und klicken Sie auf "Auswählen".

   Eine aktualisierte Liste von Benutzern, die dem Service zugewiesen sind, wird angezeigt.

6. Klicken Sie auf "Änderungen speichern".

   Der angegebene Service wird für den Benutzer durchgeführt. Der Benutzer erhält alle im Service enthaltenen Anwendungen, Rollen, Gruppen und Attribute.

Servicezuweisung bestätigen

Sobald Sie einem Benutzer einen Service zugewiesen haben, bestätigen Sie, dass alle mit dem Service verknüpften Aufgaben erfolgreich abgeschlossen wurden.

Gehen Sie wie folgt vor:

1. Wählen Sie im Navigationsmenü "Services" und "Verlauf der Service-Zugriffsanfragen anzeigen" aus.

   Ein Suchfenster wird geöffnet.

2. Suchen Sie nach dem Service, den Sie einem Benutzer zugewiesen haben.

   Um eine Liste aller Services anzuzeigen, für die Sie Administratorrechte haben, klicken Sie auf "Suchen", ohne die Suchkriterien zu ändern.

   Eine Liste von Services, die Sie verwalten können, wird angezeigt.

3. Wählen Sie den Service aus, den Sie zugewiesen haben, und klicken Sie auf "Auswählen".

   Ein Verlauf von Aktionen, die mit dem Service verknüpft sind, wird angezeigt.

4. Klicken Sie auf "Letzte Änderung", um die aktuellsten Aktionen zuerst zu sehen.

5. Bestätigen Sie, dass der Service für den entsprechenden Benutzer erfolgreich durchgeführt wurde.

6. Klicken Sie auf "Schließen".

Einen Service ändern

Als Systemadministrator können Sie einen Service ändern, den Sie zuvor erstellt haben. Zum Beispiel können Sie die Berechtigungen ändern, die der Service Servicemitgliedern gewährt, indem Sie eine Rolle zum Service hinzufügen. Sie können auch Admin- und Eigentümerregeln für den Service, Servicevoraussetzungen und andere Verwaltungsdetails anpassen.

Wenn CA CloudMinder einen Service für einen bestimmten Benutzer durchgeführt hat, werden Serviceänderungen nicht an diesen Benutzer propagiert. Wenn Sie einen Service ändern, verfügen Benutzer, für die der Service vor der Änderung durchgeführt wurde, über die ursprünglichen Berechtigungen. Benutzer, für die der Service durchgeführt wird, nachdem Sie ihn geändert haben, verfügen über die Berechtigungen, die der geänderte Service gewährt. Stellen Sie sich folgendes Beispielszenario vor:

Als Systemadministrator erstellen Sie einen Service "Vertriebs-Manager", der Servicemitgliedern die Rolle "Vertriebs-Manager" und die Gruppe "Vertrieb" gewährt. Benutzer fordern den Service "Vertriebs-Manager" an, und CA CloudMinder führt den Service durch, indem Benutzern die richtige Rolle und Gruppe gewährt wird. Sie beschließen, den Service "Vertriebs-Manager" zu ändern, um die Rolle "Mitarbeiter-Manager" einzuschließen. Vorhandene Servicemitglieder erhalten die Rolle "Mitarbeiter-Manager" dann nicht. Nur neue Mitglieder des Service "Vertriebs-Manager" erhalten die Rolle "Mitarbeiter-Manager", zusätzlich zur Rolle "Vertriebs-Manager" und zur Gruppe "Vertrieb".

Ziehen Sie ferner in Betracht, einen Service nur zu ändern, wenn er keine Mitglieder aufweist. Das heißt, ändern Sie einen Service nur, wenn kein Benutzer den Service angefordert und dieser durchgeführt wurde und kein Administrator den Service einem Benutzer zugewiesen hat.

Sie können Verwaltungsinformationen, Admin- und Eigentümerregeln, Servicevoraussetzungen und Berechtigungen – Aufgaben, Rollen, Gruppen und Attribute – für den Service ändern.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei einem CA CloudMinder-Konto mit Serviceverwaltungsberechtigungen an.

   Dem ersten Benutzer einer Umgebung ist beispielsweise die System-Manager-Rolle zugewiesen, welche die Aufgabe "Service ändern" aufweist.

2. Wählen Sie im Navigationsmenü "Services" aus.
3. Klicken Sie auf "Services verwalten" und dann "Service ändern".

   Ein Suchfenster wird geöffnet.
4. Suchen Sie nach einem Service, den Sie ändern möchten.

   Um eine Liste aller Services anzuzeigen, für die Sie Administratorrechte haben, klicken Sie auf "Suchen", ohne die Suchkriterien zu ändern.
5. Wählen Sie einen Service aus, und klicken Sie auf "Auswählen".

   Eine Bestätigungsmeldung wird angezeigt.
6. Klicken Sie auf "Ja".
7. Klicken Sie auf "Senden".

   CA CloudMinder wendet Ihre Änderungen auf den Service an.

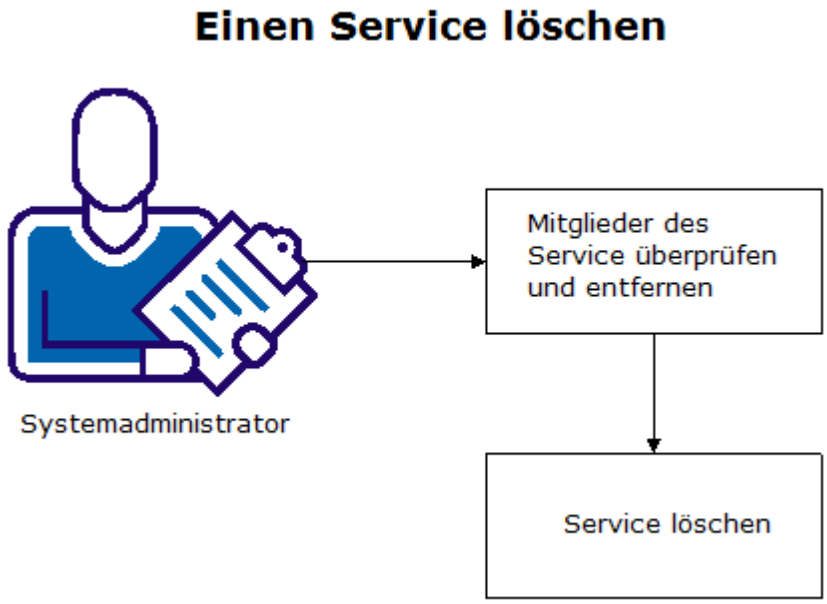
Einen Service löschen

Als Systemadministrator können Sie einen Service löschen. Ein gelöschter Service wird gänzlich aus dem System entfernt.

Wenn Benutzer einem Service zugewiesen werden, können Sie den Service nicht löschen. Bevor Sie einen Service löschen, überprüfen Sie zuerst, ob zugewiesene Benutzer oder *Mitglieder* vorhanden sind, und entfernen Sie sie.

Hinweis: Wenn ein Benutzer Mitglied eines Service ist, können Sie den Benutzer ebenfalls nicht löschen. Entfernen Sie zuerst den Benutzer als Servicemitglied, und löschen Sie dann den Benutzer.

Das folgende Diagramm zeigt alle wichtigen Informationen und die Schritte zum Löschen eines Service.



Die folgenden Themen erläutern, wie Sie einen Service löschen:

1. Servicemitglieder überprüfen und entfernen (siehe Seite 262)
2. Den Service löschen (siehe Seite 262)

Servicemitglieder überprüfen und entfernen

Bevor Sie einen Service löschen, überprüfen Sie zuerst, ob Mitglieder vorhanden sind, und entfernen Sie sie.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei einem CA CloudMinder-Konto mit Serviceverwaltungsberechtigungen an.

   Dem ersten Benutzer einer Umgebung ist beispielsweise die System-Manager-Rolle zugewiesen, welche die Aufgabe "Service ändern" aufweist.

2. Wählen Sie "Services" und "Zugriff anfordern und anzeigen".

   Eine Liste von Services, die Sie verwalten können, wird angezeigt.

3. Wählen Sie den Service aus, den Sie löschen möchten, und klicken Sie auf "Auswählen".

   Eine Liste von Benutzern, die dem Service zugewiesen sind, wird angezeigt.

4. Wenn der Service Mitglieder hat, deaktivieren Sie die Kontrollkästchen neben allen Benutzern.

5. Klicken Sie auf "Änderungen speichern".

   Eine Bestätigungsmeldung wird angezeigt.

6. Klicken Sie auf "Ja".

   CA CloudMinder entfernt die Mitglieder aus dem Service.

Einen Service löschen

Sie können einen Service löschen, der keine Servicemitglieder hat.

So löschen Sie einen Service:

1. Melden Sie sich bei einem CA CloudMinder-Konto mit Serviceverwaltungsberechtigungen an.

   Dem ersten Benutzer einer Umgebung ist beispielsweise die System-Manager-Rolle zugewiesen, welche die Aufgabe "Service ändern" aufweist.

2. Wählen Sie im Navigationsmenü "Services" aus.

3. Klicken Sie auf "Services verwalten" und "Service löschen".

   Ein Suchfenster wird geöffnet.

4. Suchen Sie den Service, den Sie löschen möchten.

   Um eine Liste aller Services anzuzeigen, für die Sie Administratorrechte haben, klicken Sie auf "Suchen", ohne die Suchkriterien zu ändern.

5. Wählen Sie einen Service aus, und klicken Sie auf "Auswählen".

   Eine Bestätigungsmeldung wird angezeigt.

6. Klicken Sie auf "Ja".

   Der Service wird gelöscht.

Erneuern des Zugriffs auf Services

Einige Services laufen nach einer gewissen Frist ab. Administratoren können einen Service erneuern, damit Benutzer ohne Unterbrechung Zugriff haben.

Sie können einen Service mithilfe einer der folgenden Methoden erneuern:

- Wählen Sie den Service aus, und wählen Sie dann den zu erneuernden Benutzerzugriff aus.
- Wählen Sie den Benutzer aus, und wählen Sie dann den zu erneuernden Service aus.

Hinweis: Je nachdem, wie eine Umgebung konfiguriert ist, können Endbenutzer ihren Zugriff auch mit der Aufgabe "Zugriff erneuern" erneuern.

Der folgende Vorgang beschreibt, wie der Zugriff erneuert wird, indem der Service zuerst ausgewählt wird. Wenn Sie zuerst den Benutzer auswählen möchten, verwenden Sie die Aufgabe "Anfragen nach Benutzerzugriff", "Benutzererneuerungsanfragen verwalten" in der Kategorie "Benutzer".

Gehen Sie wie folgt vor:

1. Klicken Sie in der Benutzerkonsole auf "Services", "Zugriff erneuern".
2. Suchen Sie den Service, den Sie erneuern möchten, und wählen Sie ihn aus.

   Die Benutzerkonsole enthält eine Liste von Benutzern, die gegenwärtig Zugriff auf den Service haben, den Sie ausgewählt haben, und das Datum, an dem ihr Zugriff abläuft.

3. Wählen Sie die Dauer für die Erneuerung in der Spalte "Zugriffsanfrage" aus, und klicken Sie dann auf "OK".

   Die Optionen im Feld "Dauer" werden bestimmt, wenn der Service erstellt wird.

4. Klicken Sie auf "Änderungen speichern".

Sie können den Status der Service-Erneuerung mit dem Verlauf der Zugriffsanfragen in der Benutzerkonsole anzeigen.

Kapitel 11: Synchronisierung

Dieses Kapitel enthält folgende Themen:

Benutzersynchronisierung zwischen Servern (siehe Seite 265)
Synchronisieren von Benutzern in Aufgaben zum Erstellen oder Ändern von Benutzern (siehe Seite 268)
Synchronisierungsaufgaben (siehe Seite 269)

Benutzersynchronisierung zwischen Servern

Sie konfigurieren die Synchronisierung in Identity Manager, um sicherzustellen, dass die Benutzerdaten im Unternehmensverzeichnis mit dem Bereitstellungsverzeichnis übereinstimmen. Damit Änderungen an einem Verzeichnis im anderen übernommen werden, konfigurieren Sie eine eingehende und ausgehende Synchronisierung.

Eingehende Synchronisierung

Die *eingehende Synchronisierung* hält die CA IdentityMinder-Benutzer bei Änderungen im Bereitstellungsverzeichnis auf dem aktuellen Stand. Änderungen im Bereitstellungsverzeichnis schließen solche mit ein, die von Systemen mit Connectors zum Bereitstellungsserver gemacht wurden. Die Synchronisierung verwendet die im Bereitstellungsfenster der Management-Konsole definierten Zuordnungen.

Failover für eingehende Synchronisierung

Ein Failover zu einer alternativen Identity Manager-Server-URL tritt nur auf, wenn der in einer URL angegebene Anwendungsserver nicht ausgeführt wird. Wenn der Anwendungsserver ausgeführt wird und die Benachrichtigung akzeptiert, dann jedoch ein Konfigurationsfehler, wie zum Beispiel eine unbekannte Umgebung oder nicht gestartete Umgebung, auftritt, blockieren diese Fehler die Übermittlung der Benachrichtigungen. Diese Probleme müssen gelöst werden, damit eingehende Benachrichtigungen ordnungsgemäß übermittelt werden.

Ausgehende Synchronisierung

Bei der *ausgehenden Synchronisierung* werden Benutzer mit Identity Manager im Bereitstellungsverzeichnis erstellt und aktualisiert.

Erstellen von globalen Benutzern mit Identity Manager

Benutzer werden im Bereitstellungsverzeichnis nur für Ereignisse im Zusammenhang mit der Bereitstellung erstellt, beispielsweise dem Zuordnen einer Bereitstellungsrolle zu einem Benutzer. Kein Benutzer wird im Bereitstellungsverzeichnis erstellt, wenn Sie eine Admin-Aufgabe verwenden, um einen Benutzer zu erstellen, außer wenn diese Aufgabe eine Rolle zuweist oder eine Identitätsrichtlinie einschließt, die die Rolle zuweist.

Wenn die Erstellung eines Benutzers in Identity Manager die Erstellung des Benutzers im Bereitstellungsverzeichnis auslöst, sendet Identity Manager eine E-Mail mit einem temporären Kennwort, das im Bereitstellungsverzeichnis festgelegt ist, an die E-Mail-Adresse des neuen Benutzers. Der Benutzer kann sich mit diesem Kennwort bei der Benutzerkonsole anmelden. Er muss es anschließend jedoch in ein neues Kennwort ändern. Daraufhin wird das Kennwort zwischen dem Benutzerspeicher und dem Bereitstellungsverzeichnis synchronisiert.

Wenn der Benutzer keine E-Mail-Adresse hat, der Benutzer erst auf die Benutzerkonsole zugreifen, wenn er das Kennwort im Benutzerspeicher geändert hat oder nachdem ein CA IdentityMinder-Administrator das Kennwort des Benutzers im Bereitstellungsmanager geändert hat.

Hinweis: Damit eine E-Mail mit dem temporären Kennwort gesendet werden kann, müssen E-Mail-Benachrichtigungen für die Umgebung aktiviert sein, und "CreateProvisioningUserNotificationEvent" muss für die E-Mail-Benachrichtigung konfiguriert sein. (Weitere Informationen finden Sie im *Konfigurationshandbuch*).

Aktualisieren von globalen Benutzern mit Identity Manager

Die Benutzer werden im Bereitstellungsverzeichnis aktualisiert, wenn Sie eine Admin-Aufgabe verwenden, die Benutzer ändert. Wenn kein globaler Benutzer vorhanden ist, erfolgt keine Synchronisierung.

Ausgehende Zuordnungen stimmen die Identity Manager-Benutzerereignisse mit einem ausgehenden Ereignis ab, das sich auf das Bereitstellungsverzeichnis auswirkt.

Identity Manager User Event	Outbound Event
☐ DeleteUserEvent	POST_DELETE_GLOBAL_USER
☐ DisableUserEvent	POST_DISABLE_GLOBAL_USER
☐ EnableUserEvent	POST_ENABLE_GLOBAL_USER
☐ ModifyUserEvent	POST_MODIFY_GLOBAL_USER
☐ ResetPasswordEvent	POST_CHANGE_GLOBAL_USER_PWD

Wenn ein Benutzer im Bereitstellungsverzeichnis, aber nicht in Identity Manager vorhanden ist, können Sie diesen Benutzer in der Benutzerkonsole erstellen. Wenn Sie Attribute für die Erstellungsaufgabe zugeordnet haben und die Benutzer die gleiche Benutzer-ID haben, werden die Attribute für den Bereitstellungsbenutzer im Bereitstellungsverzeichnis aktualisiert. Jetzt können Sie diesen Benutzer in Identity Manager verwalten.

Hinweis: Wenn ein Ereignis Benutzerattribute aktualisiert und die Werte mit CA IdentityMinder synchronisiert werden sollen, müssen Sie die Ereignisse dem ausgehenden Ereignis zuordnen: POST_MODIFY_GLOBAL_USER.

Löschen von globalen Benutzern mit Identity Manager

Standardmäßig ist die ausgehende Synchronisierung für das Ereignis "Benutzer löschen" konfiguriert. Wenn Sie einen Benutzer in Identity Manager löschen, wird er auch im Bereitstellungsverzeichnis und in allen Endpunkt-Benutzerkonten gelöscht.

Wenn CA IdentityMinder das Konto eines Benutzers an einem verwalteten Endpunkt nicht löschen kann, löscht es den Benutzer aus den verbleibenden Konten, aber nicht aus dem Bereitstellungsverzeichnis.

Angenommen, Benutzer A hat zum Beispiel ein UNIX-Konto und ein Exchange-Konto, die beide im Bereitstellungsserver verwaltet werden. Wenn Benutzer A in Identity Manager gelöscht wird, versucht der Bereitstellungsserver, die Konten des Benutzers zu löschen. Wenn der Bereitstellungsserver das Exchange-Konto aufgrund eines Kommunikationsfehlers nicht löschen kann, löscht er das UNIX-Konto von Benutzer A, aber der Benutzer wird nicht aus dem Bereitstellungsverzeichnis gelöscht. Benutzer A wird jedoch im Benutzerspeicher nicht wiederhergestellt.

Enable Password Synchronization (Kennwortsynchronisierung ermöglichen)

Der Bereitstellungsserver lässt die Kennwortsynchronisierung zwischen Identity Manager-Benutzern und zugeordneten Endpunkt-Benutzerkonten zu. Zwei Konfigurationen sind erforderlich, um auf dem Endpunkt initiierte Änderungen zu aktivieren:

- Endpunkte müssen so konfiguriert werden, dass sie die auf dem Endpunkt initiierten Änderungen erfassen und an den Bereitstellungsserver weiterleiten.

  Hinweis: Weitere Informationen zum Konfigurieren der Endpunkte für die Kennwortsynchronisierung finden sie im *CA IdentityMinder-Administrationshandbuch*.

- Der Agent zum Aktivieren der Kennwortsynchronisierung sollte für den globalen Benutzer aktiviert sein.

So aktivieren Sie die Kennwortsynchronisierung

1. Wählen Sie in der Management-Konsole "Advanced Settings" (Erweiterte Einstellungen) und "Provisioning" (Bereitstellung) aus.
2. Aktivieren Sie "Enable Password Changes from Endpoint Accounts" (Kennwortänderungen auf Endpunktkonten aktivieren).
3. Klicken Sie auf "Speichern".
4. Starten Sie den Anwendungsserver neu.

Synchronisieren von Benutzern in Aufgaben zum Erstellen oder Ändern von Benutzern

Auf der Registerkarte "Profil" einer Aufgabe, die Benutzer erstellt oder ändert, stellen Synchronisierungssteuerelemente sicher, dass Änderungen in Identity Manager auch auf den globalen Benutzer angewendet werden. Wenn Sie Admin-Aufgaben erstellen, die Benutzer erstellen oder ändern, und Identitätsrichtlinien vorhanden sind, legen Sie die Synchronisierungssteuerelemente folgendermaßen fest:

- Legen Sie "Benutzersynchronisierung" auf "Bei Abschluss der Aufgabe" fest.
- Legen Sie "Kontosynchronisierung" auf "Bei Abschluss der Aufgabe" fest.

Hinweis: Mit Auswahl der Option "Bei Abschluss der Aufgabe" werden die besten Ergebnisse erzielt. Beim Aktivieren der Option "Bei Abschluss der Aufgabe" für eine Aufgabe, die mehrere Ereignisse einschließt, führt Identity Manager die Synchronisierung allerdings erst dann durch, wenn alle Ereignisse in der Aufgabe abgeschlossen sind. Falls für eines oder mehrere Ereignisse die Genehmigung des Workflows erforderlich ist, kann dieser Prozess mehrere Tage dauern. Um zu vermeiden, dass Identity Manager mit der Anwendung der Identitätsrichtlinien oder der Kontosynchronisierung wartet, bis alle Ereignisse abgeschlossen sind, wählen Sie die Option "Bei jedem Ereignis" aus.

Wenn Sie Attribute zu Admin-Aufgaben hinzufügen, die Benutzer verwalten, müssen Sie die Attributzuordnungen im Bereitstellungsfenster in der Management-Konsole aktualisieren. Für jedes Benutzerattribut in Identity Manager ist ein Standard-Bereitstellungsattribut vorhanden.

User Attribute	Provisioning Attribute
%ADMIN_ROLE_CONSTRAINT%	%ADMIN_ROLE_CONSTRAINT%
%EMAIL%	%EMAIL%
%ENABLED_STATE%	%ENABLED_STATE%
%FIRST_NAME%	%FIRST_NAME%
%FULL_NAME%	%FULL_NAME%
%IDENTITY_POLICY%	%IDENTITY_POLICY%
%LAST_NAME%	%LAST_NAME%
%PASSWORD%	%PASSWORD%
%PASSWORD_DATA%	%PASSWORD_DATA%
%USER_ID%	%USER_ID%

Synchronisierungsaufgaben

Sie können die folgenden Synchronisierungsarten ausführen:

Benutzersynchronisierung

Stellt sicher, dass jeder Benutzer die erforderlichen Konten an den entsprechenden verwalteten Endpunkten hat, und dass jedes Konto den entsprechenden Kontovorlagen, wie von den Bereitstellungsrollen des Benutzers angegeben, zugewiesen wird.

Kontosynchronisierung

Stellt sicher, dass die Funktionsattributwerte für Konten den Werten entsprechen, die in den zugewiesenen Kontovorlagen des Kontos angegeben sind. Die Kontosynchronisierung kann stark oder schwach sein. Die schwache Synchronisierung stellt sicher, dass die Kontenfunktionsattribute über das Mindestmaß an Funktionen verfügen, die für die Kontovorlagen erforderlich sind. Die starke Synchronisierung stellt sicher, dass die Kontofunktionsattribute über die exakten Funktionen verfügen, die für die Kontovorlagen erforderlich sind. Die Kontosynchronisierung ist stark, wenn das Konto zu mindestens einer Kontovorlage gehört, deren Kontrollkästchen "Strong Synchronization" (Starke Synchronisierung) aktiviert ist.

Die Benutzersynchronisierung wird nicht durch ein entsprechendes "Strong Synchronization"-Kontrollkästchen gesteuert, aber es gibt ein ähnliches Konzept. Wenn Sie den Menüpunkt "Benutzer mit Rollen synchronisieren" auf einen Benutzer anwenden, werden zwei Synchronisierungsoptionen angezeigt:

- Sie können fehlende Konten und Kontovorlagenzuweisungen hinzufügen.
- Sie können zusätzliche Konten und Kontovorlagenzuweisungen löschen.
- Wenn Sie nur das Kontrollkästchen "Hinzufügen" auswählen - ähnlich einer schwachen Kontosynchronisierung -, möchten Sie erreichen, dass die globalen Benutzer mindestens über alle Konten verfügen, die sie für die ihnen zugewiesenen Bereitstellungsrollen benötigen. Dabei lassen Sie zu, dass die Benutzer auch über zusätzliche Konten verfügen, die für die aktuellen Bereitstellungsrollen nicht vorgeschrieben sind.

Wählen Sie die Kontrollkästchen "Hinzufügen" und "Löschen" aus - ähnlich einer starken Kontosynchronisierung -, damit die Bereitstellungsrollen genau definieren, über welche Konten der Benutzer verfügen sollte. Alle zusätzlichen Konten werden gelöscht.

Wählen Sie die schwache/starke Kontosynchronisierung oder die schwache/starke Benutzersynchronisierung abhängig davon aus, wie genau die Bereitstellungsrollen definiert sind. Wenn Ihren Benutzern klar definierte Bereitstellungsrollen zugeordnet werden können und der Kontozugriff an diese Rollen gebunden ist, verwenden Sie die starke Synchronisierung.

Hinweis: Bei einigen Endpunktarten wird die starke Synchronisierung standardmäßig festgelegt. Weitere Informationen finden Sie im *Connectors Guide*.

Bei der Benutzersynchronisierung und der Kontosynchronisierung handelt es sich um getrennte Aufgaben, die Sie einzeln ausführen müssen. Normalerweise führen Sie die Benutzersynchronisierung zuerst aus, um sicherzustellen, dass alle erforderlichen Konten erstellt werden. Sie führen die Kontosynchronisierung später aus, damit der Bereitstellungsserver die Werte der Kontoattribute zuweist oder ändert.

Der Bereitstellungsserver bietet zwei Gruppen von Synchronisierungs-Menüoptionen für Objekte:

- Mithilfe der Menüoptionen für die Synchronisierungsüberprüfung wird die Synchronisierung überprüft und eine Liste der Konten zurückgegeben, die nicht den Bereitstellungsrollen oder Kontovorlagen entsprechen.
- Mithilfe der Synchronisierungs-Menüoptionen werden globale Benutzer mit ihren Bereitstellungsrollen oder Konten mit ihren Kontovorlagen synchronisiert.

Wenn Sie die Funktionen für die Synchronisierungsüberprüfung zuerst durchführen, gibt der Bereitstellungsserver an, welche Korrekturen die Synchronisierungsfunktionen ausführen. Wenn die Funktionen für die Synchronisierungsüberprüfung kein Problem finden, werden die Synchronisierungsfunktionen nicht ausgeführt.

Gründe, warum Benutzer nicht mehr synchronisiert sind

Nachfolgend finden Sie einige Gründe, warum Benutzer nicht mehr mit ihren Bereitstellungsrollen oder Kontovorlagen synchronisiert sind:

- Frühere Versuche, die erforderlichen Konten zu erstellen, schlugen aufgrund von Hardware- oder Softwareproblemen in Ihrem Netzwerk fehl, was zu fehlenden Konten führte.
- Bereitstellungsrollen und Kontovorlagen können sich geändert haben, wodurch zusätzliche oder fehlende Konten entstanden sind.
- Konten wurden Kontovorlagen nach ihrer Erstellung zugewiesen. Das heißt, es sind Konten vorhanden, die nicht mit ihren Kontovorlagen synchronisiert wurden.
- Die Erstellung eines neuen Kontos wird verschoben, da die Kontoerstellung auf einen späteren Zeitpunkt festgelegt wurde.
- Ein neuer Endpunkt wurde erworben. Während der Durchsuchung und Korrelation weist der Bereitstellungsserver den Benutzern nicht automatisch Bereitstellungsrollen zu. Das heißt, dass Sie die Rolle aktualisieren müssen, um anzugeben, welche Benutzer Konten auf dem neuen Endpunkt haben sollen. Ein Konto, das zu einem Benutzer korreliert wurde, wird bei der Synchronisierung des Benutzers als zusätzliches Konto aufgelistet.
- Ein vorhandenes Konto wurde einem Benutzer durch Kopieren des Kontos zugewiesen, wodurch eine manuelle Korrelation durchgeführt und ein zusätzliches Konto eingerichtet wurde.
- Ein Konto wurde nicht durch Zuweisen des Benutzers zu einer Rolle für einen Benutzer erstellt. Wenn Sie zum Beispiel einen Benutzer in eine Kontovorlage kopieren, die in keiner der Bereitstellungsrollen des Benutzers vorhanden ist, wird das Konto als zusätzliches Konto oder als Konto mit einer zusätzlichen Kontovorlage aufgelistet. Wenn Sie den Benutzer zu einem Endpunkt kopieren, um mit der Standardkontovorlage des Endpunkts ein Konto zu erstellen, könnte es sich bei diesem Konto um ein zusätzliches Konto handeln.

Benutzersynchronisierung

Die Benutzersynchronisierung erstellt, aktualisiert oder löscht Konten, damit sie der Bereitstellungsrolle entsprechen, die einem Benutzer zugewiesen wurde. Wenn also Administratoren Konten an Ihrem verwalteten Endpunkt mithilfe von systemeigenen Tools hinzufügen oder löschen und Sie keine erneute Durchsuchung Ihres Endpunkts durchgeführt haben, um das Bereitstellungsverzeichnis zu aktualisieren, gibt die Benutzersynchronisierung möglicherweise an, dass keine Probleme vorhanden sind, obwohl ein Benutzer zusätzliche oder fehlende Konten hat.

Synchronisierung von Benutzern mit Rollen

Sie können die Synchronisierung für Benutzer überprüfen, um zusätzliche Konten oder Kontovorlagen und fehlende Konten aufzulisten. Wenn Sie die Synchronisierung von Benutzern mit Rollen anfordern, stellt der Bereitstellungsserver sicher, dass der Benutzer alle für seine Bereitstellungsrollen erforderlichen Konten hat und dass jedes Konto zu den richtigen Kontovorlagen gehört.

- Mit dieser Aufgabe können Sie ein Kontrollkästchen aktivieren, um das Konto auf dem Endpunkt zu erstellen. Wenn mehr als eine Kontovorlage in den Bereitstellungsrollen des Benutzers das gleiche Konto vorschreibt, wird das Konto durch das Zusammenführen aller relevanten Kontovorlagen erstellt.
- Während der Synchronisierung von Benutzern mit Rollen haben Sie die Option, zusätzliche Konten zu löschen. Möglicherweise gibt es gute Gründe, warum die Benutzer zusätzliche Konten haben, die für ihre Bereitstellungsrollen nicht erforderlich sind. In dem Fall sollten Sie diese Löschoption nicht aktivieren.

  Wenn ein Konto, das gelöscht wird, sich in einem verwalteten Endpunkt befindet, für den Kontolöschungen deaktiviert worden sind, wird das Konto nicht wirklich gelöscht.

Erstellen von Konten

Da Bereitstellungsrollen Kontovorlagen enthalten und Kontovorlagen Endpunkten zugeordnet sind, sollten die Konten für den Benutzer auf jedem Endpunkt mit den richtigen Kontoattributen aufgeführt sein.

Mit dieser Aufgabe können Sie ein Kontrollkästchen aktivieren, um das Konto auf dem Endpunkt zu erstellen. Wenn mehr als eine Kontovorlage in den Bereitstellungsrollen des Benutzers das gleiche Konto vorschreibt, wird das Konto durch das Zusammenführen aller relevanten Kontovorlagen erstellt.

Dieses Konto wird den Kontovorlagen zugewiesen, die gegenwärtig nicht mit dem Konto synchronisiert sind. Kontosynchronisierung ist auf neu erstellten Konten nicht notwendig.

Löschen von Konten

Während der Synchronisierung von Benutzern mit Rollen haben Sie die Option, zusätzliche Konten zu löschen. Möglicherweise gibt es gute Gründe, warum die Benutzer zusätzliche Konten haben, die für ihre Bereitstellungsrollen nicht erforderlich sind. In dem Fall sollten Sie diese Löschoption nicht aktivieren.

Wenn ein Konto, das gelöscht wird, sich in einem verwalteten Endpunkt befindet, für den Kontolöschungen deaktiviert worden sind, wird das Konto nicht wirklich gelöscht.

Hinzufügen von Kontovorlagen zu Konten

Wenn für ein Konto eine oder mehrere Kontovorlagenzuweisungen fehlen, weist der Benutzer mit Kontovorlagensynchronisierung diesen Kontovorlagen ein vorhandenes Konto zu. Wenn ein Konto einer oder mehreren neuen Kontovorlagen zugewiesen wird, wird die Kontosynchronisierung automatisch ausgeführt, um die Funktionsattribute des Kontos mit den in den Kontovorlagen angegebenen Funktionen zu aktualisieren.

Nachdem das Konto vom Benutzer mit Kontovorlagensynchronisierung aktualisiert wurde, sind das Konto und die entsprechenden Kontovorlagen möglicherweise synchronisiert. Wenn eine der hinzugefügten Kontovorlagen eine Kontovorlage mit starker Synchronisierung war oder wenn mindestens zwei Kontovorlagen zu einem Konto hinzugefügt wurden, startet der Benutzer mit Rollensynchronisierung eine vollständige Kontosynchronisierung für das Konto. Wenn jedoch nur eine Kontovorlage mit schwacher Synchronisierung hinzugefügt wurde, wird bei der Benutzersynchronisierung mit der Kontovorlagensynchronisierung eine Kontosynchronisierung gestartet, die nur diese eine Kontovorlage umfasst. Wenn das Konto vor dieser Aktualisierung bisher nicht an der Kontosynchronisierung mit seinen anderen Kontovorlagen beteiligt war, ist dies möglicherweise auch nach der Aktualisierung der Fall.

Entfernen von Kontovorlagen aus Konten

Der Benutzer mit Rollensynchronisierung kann auch verwendet werden, um zusätzliche Kontovorlagen aus einem Konto zu entfernen. Dies wird nur durchgeführt, wenn Sie die Löschoption aktivieren. Wenn bei der Benutzersynchronisierung festgestellt wird, dass ein Konto aktualisiert werden muss, um eine oder mehrere zusätzliche Kontovorlagen zu entfernen, wird die Kontosynchronisierung automatisch für das Konto ausgeführt, um seine Funktionsattribute mit den Kontovorlagen zu synchronisieren, die im Konto verbleiben.

Diese Kontosynchronisierung, die beim Entfernen von Kontovorlagen aus einem Konto durchgeführt wird, verwendet die starke Synchronisierung, wenn für eine der verbleibenden Kontovorlagen die starke Synchronisierung angegeben ist, und die schwache Synchronisierung, wenn für alle verbleibenden Kontovorlagen die schwache Synchronisierung angegeben ist.

Die Entscheidung, ob die schwache oder die starke Synchronisierung verwendet wird, beeinflusst, ob Kontofunktionen, die zuvor bei der Zuweisung der Kontovorlage zu einem Konto erteilt wurden, entfernt werden, wenn diese Kontovorlage später entfernt wird. Bei der starken Synchronisierung wird eine Funktion, die von einer Kontovorlage erteilt wurde - beispielsweise eine Gruppenmitgliedschaft oder ein höheres Kontingent - entfernt (Gruppenmitgliedschaft entfernt oder das Kontingent verringert), wenn keine der im Konto verbleibenden Kontovorlagen diese Funktion vorschreiben. Bei der schwachen Synchronisierung bleibt das Konto jedoch normalerweise unverändert, weil der Bereitstellungsserver nicht zwischen zusätzlichen On-Demand-Funktionen und durch Kontovorlagen erteilte Funktionen unterscheidet.

Die Ausnahme zu dieser Regel bilden bestimmte Funktionsattribute mit mehreren Werten, die als SyncRemoveValues-Attribute festgelegt sind. Ein einfaches Attribut mit mehreren Werten, das eine Sammlung von Werten darstellt, die dem Konto zugewiesen sind (beispielsweise eine Gruppenmitgliedschaftsliste), wird in der Regel als SyncRemoveValues-Attribut aufgelistet. Bei diesen Attributen entfernt die schwache Synchronisierungsaktion, die beim Entfernen einer Kontovorlage aus einem Konto durchgeführt wird, von der entfernten Kontovorlage vorgeschriebene Werte - sofern diese Werte nicht auch von einer der verbleibenden Kontovorlagen vorgeschrieben werden.

Wenn Sie zum Beispiel Ihre Kontovorlagen erstellen und jede Kontovorlage Ihrem Konto eine eindeutige Gruppenmitgliedschaft zuweist, bewirkt diese SyncRemoveValues-Funktion, dass bei einer Änderung der Bereitstellungsrollen eines globalen Benutzers, die zur Folge hat, dass eine bestimmte Kontovorlage nicht mehr erforderlich ist, das Konto aktualisiert wird und nicht mehr zu der von dieser Kontovorlage vorgeschriebenen Gruppe gehört. Dies ist nicht genau das Gleiche wie eine starke Synchronisierung, da Gruppenmitgliedschaften, die Konten erteilt wurden und über die von den Kontovorlagen vorgeschriebenen Werte hinausgehen, beibehalten werden.

Bei allen Attributen mit einem Wert und bestimmten Attributen mit mehreren Werten, die nicht als SyncRemoveValues-Attribute festgelegt sind, entspricht die schwache Synchronisierungsaktion beim Entfernen einer Kontovorlage aus einem Konto der normalen schwachen Synchronisierungsaktion - Funktionen werden nie entfernt.

Wenn Funktionen bei der schwachen Synchronisierung nie entfernt werden sollen, deaktivieren Sie die SyncRemoveValues-Funktion, indem Sie den Domänenkonfigurationsparameter "Synchronize/Remove Account Template Values from Accounts" (Kontenvorlagenwerte synchronisieren oder aus Konten entfernen) auf "Nein" setzen.

Synchronisierung von Kontovorlagen

Änderungen, die Sie an Kontovorlagen vornehmen, wirken sich folgendermaßen auf bestehende Konten aus:

- Wenn Sie den Wert eines Funktionsattributs ändern, wird das entsprechende Kontoattribut bei Bedarf aktualisiert, damit die Übereinstimmung mit dem Kontovorlagen-Attributwert sichergestellt ist. Weitere Informationen hierzu finden Sie in der Beschreibung von schwacher und starker Synchronisierung.
- Bei bestimmten Kontoattributen wird vom Connector festgelegt, dass sie bei einer Kontovorlagen-Änderung nicht aktualisiert werden sollen. Beispiele sind bestimmte Attribute, deren Festlegung der Endpunkttyp nur während der Kontoerstellung zulässt, und das Kennwort-Attribut.

Synchronisierung von Funktionsattributen

Wenn Sie Funktionsattribute in einer Kontovorlage ändern, ändern sich ggf. auch die entsprechenden Attribute in den Konten. Ob die Attribute eines jeweiligen Kontos betroffen sind, ist von zwei Faktoren abhängig:

- ob die Kontovorlage für die Verwendung schwacher oder starker Synchronisierung definiert ist
- ob das Konto mehreren Kontovorlagen zugeordnet ist

Schwache Synchronisierung

Schwache Synchronisierung stellt sicher, dass Benutzer über das Mindestmaß an Funktionsattributen verfügen, das ihre Konten aufweisen sollten. Schwache Synchronisierung ist der Standard für die meisten Endpunkttypen. Wenn Sie eine Vorlage aktualisieren, die schwache Synchronisation verwendet, aktualisiert CA IdentityMinder Funktionsattribute folgendermaßen:

- Wenn ein numerisches Feld in einer Kontovorlage aktualisiert wird und der neue Zahlenwert höher als der im Konto vorhandene Wert ist, übernimmt CA IdentityMinder den neuen Wert für das Konto.
- Wenn bei einer Kontovorlage das Kontrollkästchen nicht ausgewählt war und Sie es nachträglich auswählen, aktualisiert CA IdentityMinder das Kontrollkästchen bei allen Konten, bei denen es nicht ausgewählt ist.
- Wenn eine Liste in einer Kontovorlage geändert wird, aktualisiert CA IdentityMinder alle Konten dahin gehend, dass neue Werte in der Liste, die in der im Konto vorhandenen Liste nicht vorhanden sind, hinzugefügt werden.

Falls ein Konto anderen Kontovorlagen zugeordnet ist (unabhängig davon, ob die entsprechenden Vorlagen schwache oder starke Synchronisierung nutzen), berücksichtigt CA IdentityMinder nur die geänderte Vorlage. Diese Aktion ist effizienter als eine Überprüfung aller Kontovorlagen. Da bei der schwachen Synchronisierung nur Funktionalitäten zu Konten hinzugefügt werden, ist es in der Regel nicht erforderlich, die anderen Kontovorlagen zu überprüfen.

Hinweis: Bei der Propagierung auf der Grundlage einer Kontovorlage mit schwacher Synchronisierung werden Änderungen, bei denen Funktionalitäten entfernt oder eingeschränkt werden, möglicherweise für einige Konten nicht übernommen. Denken Sie daran, dass bei Verwendung schwacher Synchronisierung niemals Funktionalitäten entfernt oder eingeschränkt werden. Wenn keine weiteren Vorlagen für ein Konto geprüft werden, kann bei der Propagierung nicht berücksichtigt werden, ob eine schwache Synchronisierung ausreicht.

Verwenden Sie in dieser Situation "Benutzer mit Kontovorlagen synchronisieren", um das Konto mit den zugehörigen Kontovorlagen zu synchronisieren.

Starke Synchronisierung

Eine starke Synchronisierung stellt sicher, dass Konten genau die in der Kontovorlage angegebenen Kontoattribute aufweisen.

Beispiel: Sie fügen eine Gruppe zu einer vorhandenen UNIX-Kontovorlage hinzu. Ursprünglich generierte die Kontovorlage Kontenmitglieder der Gruppe "Mitarbeiter". Jetzt möchten Sie Kontenmitglieder für die Gruppen "Mitarbeiter" und "System" generieren. Alle der Kontovorlage zugeordneten Konten werden als synchronisiert betrachtet, wenn jedes Konto Mitglied der Gruppen "Mitarbeiter" und "System" ist (und keiner anderen Gruppen). Konten, die nicht zur Gruppe "Mitarbeiter" gehören, werden beiden Gruppen hinzugefügt.

Folgende andere Faktoren müssen u. a. berücksichtigt werden:

- Wenn die Kontovorlage die starke Synchronisierung verwendet, werden Konten, die zu anderen Gruppen gehören als "Mitarbeiter" und "System", aus diesen zusätzlichen Gruppen entfernt.
- Wenn die Kontovorlage die schwache Synchronisierung verwendet, werden die Konten den Gruppen "Mitarbeiter" und "System" hinzugefügt. Jedes Konto, für das zusätzliche Gruppen definiert sind, bleibt Mitglied dieser Gruppen.

Hinweis: Synchronisieren Sie Konten regelmäßig mit den entsprechenden Vorlagen, um sicherzustellen, dass sie synchronisiert bleiben.

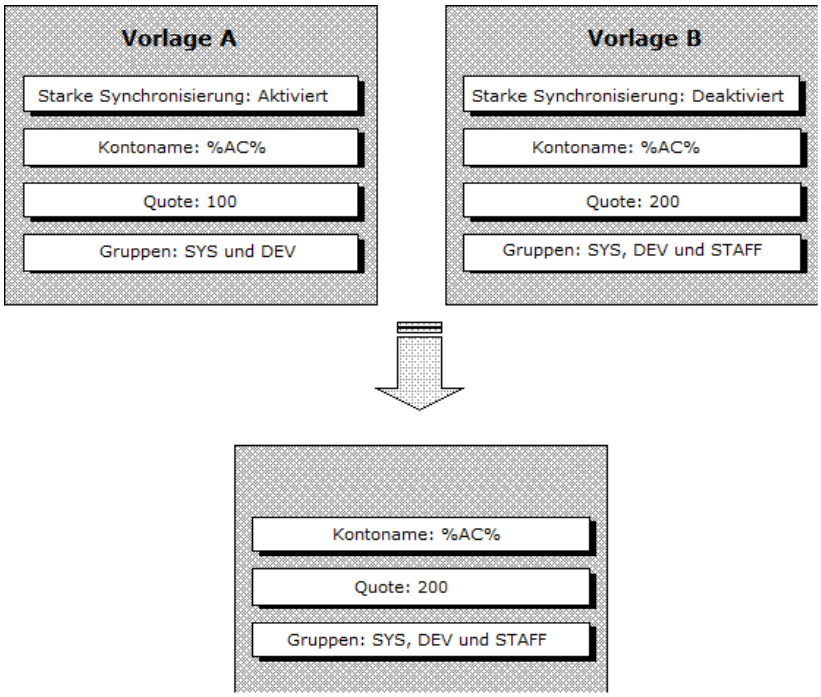
Konten mit mehreren Vorlagen

Die Synchronisierung hängt auch davon ab, ob das Konto zu mehr als einer Kontovorlage gehört. Wenn ein Konto nur eine Kontovorlage aufweist und diese Vorlage die starke Synchronisierung verwendet, wird jedes Attribut aktualisiert, um genau mit dem Kontovorlage-Attributwert übereinzustimmen. Das Ergebnis entspricht dem eines anfänglichen Attributs.

Ein Konto kann zu mehreren Kontovorlagen gehören, beispielsweise wenn ein globaler Benutzer zu mehreren Bereitstellungsrollen gehört, von denen jede ein bestimmtes Maß an Zugriff auf denselben verwalteten Endpunkt vorschreibt. In diesem Fall kombiniert CA IdentityMinder diese Kontovorlagen in einer gültigen Kontovorlage, die die Obermenge an Funktionen aus den einzelnen Kontovorlagen vorschreibt. Diese Kontovorlage verwendet die schwache Synchronisierung, wenn alle einzelnen Kontovorlagen diese Synchronisierung verwenden, oder die starke Synchronisierung, wenn eine der Kontovorlagen diese Synchronisierung verwendet.

Hinweis: In der Regel verwenden Sie entweder die schwache oder starke Synchronisierung für die Kontovorlagen für ein Konto, je nach dem, ob Ihre Unternehmensrollen den Zugriff, den Ihre Benutzer benötigen, komplett definieren. Wenn Ihren Benutzer keine klaren Rollen zugeordnet werden können und Sie den Konten Ihrer Benutzer zusätzliche Funktionen gewähren müssen, verwenden Sie die schwache Synchronisierung. Wenn Sie Rollen definieren können, um genau den Zugriff anzugeben, den Ihre Benutzer benötigen, verwenden Sie die starke Synchronisierung.

Das folgende Beispiel demonstriert, wie mehrere Kontovorlagen in einer einzelnen gültigen Kontovorlage kombiniert werden. In diesem Beispiel wird für eine Kontovorlage die schwache Synchronisierung und die andere Vorlage die starke Synchronisierung festgelegt. Daher wird die gültige Kontovorlage (eine Kombination aus den beiden Kontovorlagen) als Kontovorlage mit starker Synchronisierung behandelt. Das Attribut "Kontingent" (Ganzzahl) übernimmt den größeren Wert aus den beiden Kontovorlagen und das Attribut "Gruppen" (mehrwertig) übernimmt beide Werte aus den Richtlinien.



Attribute, mit denen nur neue Konten versehen werden

Bestimmte Attribute einer Kontovorlage werden nur bei der Erstellung eines Kontos angewendet. So ist beispielsweise das Kennwort-Attribut ein Regelausdruck, der das Kennwort für neue Konten definiert. Dieser Regelausdruck aktualisiert niemals das Kennwort eines Kontos. Änderungen hinsichtlich des Kennwort-Regelausdrucks betreffen nur nach dem Festlegen des Regelausdrucks erstellte Konten.

In ähnlicher Weise betrifft ein Vorlagen-Regelausdruck für ein schreibgeschütztes Kontoattribut nur Konten, die nach dem Festlegen dieses Regelausdrucks erstellt werden. Eine Änderung dieses Ausdrucks hat keine Auswirkungen auf vorhandene Konten.

Kontosynchronisierung

Die Kontosynchronisierung aktualisiert Funktionsattribute, um sicherzustellen, dass das Konto die von den Kontovorlagen angegebenen Funktionen aufweist. Diese Synchronisierung beeinflusst die anfänglichen Attribute des Kontos nicht.

Um Änderungen an den Funktionsattributen in einer Kontovorlage mit den entsprechenden Konten zu synchronisieren, verwenden Sie eine der in diesem Abschnitt beschriebenen Synchronisierungs-Menüoptionen.

Überprüfen der Kontosynchronisierung

Sie können die Kontosynchronisierung für Endpunkte und Benutzer überprüfen. Diese Aktion gibt eine Liste mit Konten zurück, die den Kontovorlagen nicht entsprechen. In der folgenden Tabelle werden die Vorgänge bei der Überprüfung der Kontosynchronisierung für jedes Objekt beschrieben:

Objekt	Synchronisiert
Endpunkt	Kontenattribute für jedes Konto auf einem Endpunkt und stellt sicher, dass sie den zugeordneten Kontovorlagen entsprechen.
Globaler Benutzer	Kontenattribute für jedes der Benutzerkonten und stellt sicher, dass sie den zugeordneten Kontovorlagen entsprechen.

Synchronisieren von Konten

Sie können die Kontosynchronisierung für Endpunkte, Benutzer und Kontovorlagen ausführen. In der folgenden Tabelle werden die Auswirkungen der Kontoüberprüfung für jedes Objekt beschrieben:

Objekt	Synchronisiert
Endpunkt	Jedes Konto auf einem Endpunkt mit den zugeordneten Kontovorlagen.
Globaler Benutzer	Jedes Konto eines globalen Benutzers mit jeder zugeordneten Kontovorlage.

Kapitel 12: Workflow

Dieses Kapitel enthält folgende Themen:

Workflow-Übersicht (siehe Seite 281)
Verwenden der Workflow-Kontrolle - Vorlagenmethode (siehe Seite 284)
Verwenden der WorkPoint-Methode (siehe Seite 304)
Workpoint-Job-Ansicht (siehe Seite 337)
Richtlinienbasierter Workflow (siehe Seite 340)
Online-Anfragen (siehe Seite 362)
Schaltflächen für Workflow-Aktionen (siehe Seite 366)
Arbeitslisten und Arbeitselemente (siehe Seite 371)

Workflow-Übersicht

Mit der CA IdentityMinder Workflow-Funktion kann eine CA IdentityMinder Aufgabe von einem Workflow-Prozess gesteuert werden. Ein *Workflow-Prozess* besteht aus einem oder mehreren Schritten, die durchgeführt werden müssen, bevor CA IdentityMinder eine Aufgabe abschließen kann, die der Workflow-Kontrolle unterliegt. Ein *Job* ist eine Laufzeitinstanz eines Workflow-Prozesses.

WorkPoint Designer ist eine in CA IdentityMinder integrierte Software von Workpoint LLC, einer Tochtergesellschaft von Planet Group, Inc. Mit WorkPoint Designer können Sie Workflow-Prozesse und Workflow-Jobs verwalten.

Ein Workflow-Prozess besteht aus einem oder mehreren Schritten, sogenannten *Aktivitäten*, die durchgeführt werden müssen, damit einige Geschäftsaufgaben, wie das Erstellen oder Ändern eines Arbeitnehmerkontos, abgeschlossen werden können. Im Allgemeinen umfasst ein Workflow-Prozess eine oder mehrere manuelle Aktivitäten, für die ein autorisierter Benutzer oder Teilnehmer die Aufgabe genehmigen oder ablehnen muss.

Ein *Teilnehmer* ist eine Person, die zur Durchführung einer Workflow-Aktivität berechtigt ist. In CA IdentityMinder werden Teilnehmer auch *Genehmiger* genannt, da sie die der Workflow-Kontrolle unterliegende Aufgabe genehmigen oder ablehnen müssen. Ein *Teilnehmer-Resolver* ist eine Regel oder eine Reihe von Kriterien zur Feststellung der Teilnehmer.

Die einzelnen manuellen Aktivitäten im Workflow werden in CA IdentityMinder *Arbeitselemente* genannt.

Eine *Arbeitsliste* ist eine vom Workflow generierte Liste von Genehmigungsaufgaben oder *Arbeitselementen*, die in der Benutzerkonsole des Teilnehmers angezeigt wird, der zur Genehmigung der Aufgabe berechtigt ist.

WorkPoint-Prozessdiagramm

Im Allgemeinen lösen CA IdentityMinder-Aufgaben CA IdentityMinder-Ereignisse aus. Um beispielsweise einen Benutzer zu erstellen, wählt ein Administrator eine Aufgabe "Benutzer erstellen". Bei Beginn dieser Aufgabe wird das Ereignis CreateUserEvent ausgelöst.

Das nachstehende Diagramm ist ein Beispiel für einen einfachen Workflow-Prozess (den vordefinierten Prozess CreateUserApproveProcess), wie er in WorkPoint Designer zu finden ist. Dieser Prozess wird von einem Ereignis CreateUserEvent aufgerufen, wenn die Aufgabe "Benutzer erstellen" der Workflow-Kontrolle unterliegt.

Der Prozess beinhaltet eine manuelle Aktivität, "Bestätigen: Benutzer erstellen", die einer Workflow-Genehmigungsaufgabe desselben Namens in CA IdentityMinder entspricht. Bevor die der Workflow-Kontrolle unterliegende Aufgabe abgeschlossen werden kann, muss der Teilnehmer die Genehmigungsaufgabe genehmigen oder ablehnen. Dies geschieht im Allgemeinen durch Klicken auf eine Schaltfläche in der Benutzerkonsole.

Workflow und E-Mail-Benachrichtigung

Wenn Sie eine Aufgabe initiieren, sendet CA IdentityMinder die Aufgabe zur Verarbeitung und zeigt folgende Bestätigungsmeldung an:

```
Bestätigung: Aufgabe abgeschlossen.
```

Wenn die Aufgabe jedoch der Workflow-Kontrolle unterliegt und genehmigt werden muss, gestaltet sich die Meldung wie folgt:

```
Alarm: Aufgabe steht aus.
```

Neben auf dem Bildschirm angezeigten Meldungen können in CA IdentityMinder in den folgenden Fällen automatisch E-Mail-Benachrichtigungen generiert werden:

- Ein Ereignis oder eine Aufgabe, das bzw. die von einem Workflow-Genehmiger genehmigt oder abgelehnt werden muss, ist ausstehend.
- Ein Genehmiger genehmigt ein Ereignis oder eine Aufgabe.
- Ein Genehmiger lehnt ein Ereignis oder eine Aufgabe ab.
- Ein Ereignis oder eine Aufgabe wird abgeschlossen.

Weitere Informationen:

E-Mail-Benachrichtigungen (siehe Seite 385)

WorkPoint-Dokumentation

Allgemeine Informationen zu Workflow-Konzepten und Anweisungen zu Workflow-Prozessen, -Aktivitäten und -Jobs in WorkPoint Designer finden Sie in der WorkPoint-Dokumentation. Öffnen Sie hierzu die folgende HTML-Seite:

admin_tools\WorkPoint\docs\designer\default.htm

admin_tools

Definiert das Installationsverzeichnis der CA IdentityMinder-Verwaltungstools. Das Standard-Installationsverzeichnis lautet:

- **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

Hinweis: Workpoint ist ein Drittanbieter-Produkt, das mit CA IdentityMinder installiert wird. CA IdentityMinder unterstützt eine Teilmenge der Funktionalität in WorkPoint. Beispielsweise unterstützt CA IdentityMinder die WpConsole nicht. Allerdings beschreibt die WorkPoint-Dokumentation alle Funktionen im Produkt. Teile der Workpoint-Dokumentation gelten nicht für CA IdentityMinder-Benutzer.

Workflow-Steuermethoden

In CA IdentityMinder können Aufgaben auf zwei Arten der Workflow-Kontrolle unterstellt werden:

Vorlagenmethode

CA IdentityMinder enthält Vorlagen für Workflow-Prozesse, mit denen Sie Aufgaben der Workflow-Kontrolle unterstellen können. Mit der *Vorlagenmethode* können Sie den Workflow mit Hilfe dieser Vorlagen vollständig über die Benutzerkonsole konfigurieren und verwalten. Diese in CA IdentityMinder r12 eingeführten generischen Prozessvorlagen können für die Steuerung der meisten CA IdentityMinder-Aufgaben konfiguriert werden.

Die Vorlagenmethode bietet folgende neuen Funktionen:

- Workflow-Kontrolle sowohl auf Aufgaben- als auch auf Ereignisebene
- Vereinfachte Konfiguration der Teilnehmer-Resolver für Workflow-Genehmiger
- Delegierung von Arbeitselementen auch außerhalb des Büros, wobei ein Benutzer die Erlaubnis erhält, die Genehmigung von Arbeitselementen an einen anderen Benutzer zu delegieren
- Neuzuweisung von Arbeitselementen, wobei eine laufende Aufgabe einem anderen Benutzer zur Genehmigung zugewiesen werden kann

WorkPoint-Methode

CA IdentityMinder enthält außerdem eine Reihe vordefinierter Workflow-Prozesse mit Standard-Ereigniszuordnungen, die bestimmten CA IdentityMinder-Aufgaben entsprechen. Bei der *WorkPoint-Methode* müssen Sie diese Prozesse in WorkPoint Designer konfigurieren und anpassen. Diese vordefinierten Prozesse sind mit Versionen vor CA IdentityMinder r12 kompatibel.

Die WorkPoint-Methode bietet außerdem folgende neue Funktionen:

- Workflow-Kontrolle sowohl auf Aufgaben- als auch auf Ereignisebene
- Delegierung von Arbeitselementen auch außerhalb des Büros, wobei ein Benutzer die Erlaubnis erhält, die Genehmigung von Arbeitselementen an einen anderen Benutzer zu delegieren
- Neuzuweisung von Arbeitselementen, wobei eine laufende Aufgabe einem anderen Benutzer zur Genehmigung zugewiesen werden kann

Hinweis: Für mehr Flexibilität und Benutzerfreundlichkeit empfiehlt CA, die Vorlagen-Methode wann immer möglich zu verwenden.

Weitere Informationen:

Verwenden der Workflow-Kontrolle - Vorlagenmethode (siehe Seite 284)

Verwenden der Workflow-Kontrolle - Vorlagenmethode

Die in CA IdentityMinder r12 eingeführte Vorlagenmethode ermöglicht Ihnen das Konfigurieren von Workflow-Prozessvorlagen in der Benutzerkonsole, ohne dass Sie WorkPoint Designer öffnen müssen.

Die Vorlagenmethode bietet die folgenden Vorteile:

- Mehrstufige Prozessvorlagen werden den meisten Workflow-Anforderungen gerecht, wodurch keine Anpassungen in WorkPoint Designer vorgenommen werden müssen.
- Vorlagen unterstützten die Workflow-Kontrolle sowohl auf Aufgaben- als auch auf Ereignisebene.
- Eine Workflow-Prozessvorlage kann zur Verwendung mit vielen verschiedenen Aufgaben konfiguriert werden, während die Beschaffenheit des Prozesses selbst unverändert bleibt.
- Teilnehmer-Resolver können einfach in der Benutzerkonsole festgelegt werden.
- Die Delegierung von Arbeitselementen kann in der Benutzerkonsole erfolgen.

Voraussetzung: Workflow aktivieren

Der Workflow muss aktiviert werden, bevor Sie ihn zur Steuerung von CA IdentityMinder-Aufgaben verwenden können. Standardmäßig ist der Workflow deaktiviert.

Gehen Sie wie folgt vor:

1. Wählen Sie in der Managementkonsole eine Umgebung aus.
2. Wählen Sie "Erweiterte Einstellungen", "Workflow".
3. Aktivieren Sie das Kontrollkästchen "Aktiviert" und klicken Sie auf "Speichern".

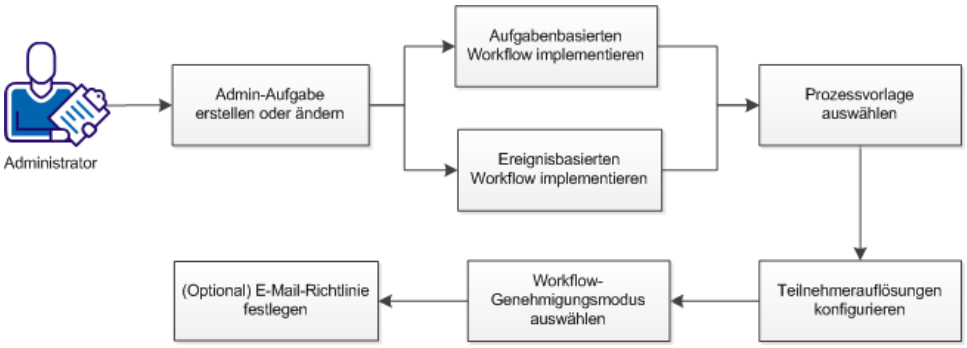
   Hinweis: Die Ereigniszuordnungen in diesem Fenster gelten nur, wenn Sie den Workflow mit der WorkPoint-Methode konfigurieren. Wenn Sie die Vorlagenmethode (empfohlen) verwenden, ordnen Sie in dieser Management-Konsole Prozessen keine Ereignisse zu.
4. Starten Sie den Anwendungsserver neu.
5. (Optional) Konfigurieren Sie die WorkPoint-Verwaltungstools (siehe Seite 306).

Weitere Informationen:

Globales Zuordnen von Prozessen zu Ereignissen (siehe Seite 314)
Workflow-Steuermethoden (siehe Seite 283)

Stellen von Admin-Aufgaben unter Workflow-Kontrolle - Vorlagenmethode

Als Administrator können Sie Admin-Aufgaben mithilfe der Vorlagenmethode der Workflow-Kontrolle unterstellen.



Gehen Sie wie folgt vor:

1. Wählen Sie in der Benutzerkonsole die Optionen "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe ändern" oder "Admin-Aufgabe erstellen" aus.
2. Suchen Sie die Aufgabe, die Sie der Workflow-Kontrolle unterstellen möchten, und klicken Sie auf "Auswählen".
3. Führen Sie *einen* der folgenden Schritte aus:
   - Implementieren Sie den Workflow auf Aufgabenebene (siehe Seite 287), indem Sie auf der Registerkarte "Profil" auf die Schaltfläche zum Bearbeiten des Workflow-Prozesses klicken.
   - Implementieren Sie den Workflow auf Ereignisebene (siehe Seite 290), indem Sie auf der Registerkarte "Ereignisse" ein oder mehrere Ereignisse auswählen.
4. Wählen Sie eine Prozessvorlage aus (siehe Seite 293).
5. Konfigurieren Sie Teilnehmerauflösungen (siehe Seite 297).
6. Wählen Sie den Workflow-Genehmigungsmodus aus.
7. (Optional) Legen Sie eine E-Mail-Richtlinie für den Workflow-Prozess fest (siehe Seite 302).

   Hinweis: Wenn Sie den EscalationApproval-Prozess auswählen, wird ein Feld mit der Bezeichnung "Genehmigungs-Timeout (min)" angezeigt. Der Wert dieses Felds wird in Minuten angegeben, das Feld darf nicht leer sein. Standardmäßig sind für dieses Zeitlimit 60 Minuten festgelegt.

Nach der Konfigurierung der Workflow-Kontrolle führt ein Benutzer mit der entsprechenden Rolle die Admin-Aufgabe aus, und die Aufgabe oder das Ereignis wird von dem festgelegten Workflow-Teilnehmer genehmigt oder abgelehnt.

Aufgaben- oder ereignisbasierter Workflow

In CA IdentityMinder können Sie Workflow-Prozesse mit Aufgaben oder Ereignissen verbinden. Dies bedeutet, dass die Teilnehmer eine ganze CA IdentityMinder-Aufgabe oder ein spezielles Ereignis in einer Aufgabe genehmigen oder ablehnen können.

So werden beispielsweise von manchen CA IdentityMinder-Aufgaben mehrere Ereignisse generiert und der Genehmiger muss möglicherweise erst alle Ereignisse überprüfen, bevor er beschließt, eine Anforderung zu genehmigen oder abzulehnen. Dies kann in einem Workflow auf Aufgabenebene erfolgen. Wenn ein Workflow-Prozess mit einem bestimmten Ereignis in einer Aufgabe verbunden ist, kann der Genehmiger den gesamten Aufgabenkontext, in dem eine Anforderung gestellt wird, nicht sehen.

Workflow auf Aufgabenebene

Der Workflow auf Aufgabenebene ermöglicht es dem Genehmiger, alle Ereignisse zu überprüfen, bevor er beschließt, eine Anforderung zu genehmigen oder abzulehnen. Der Workflow auf Aufgabenebene findet vor der Verarbeitung von Aufgabenaktivitäten statt. Vor Beginn des Workflow-Prozessjobs werden keinerlei Ereignisse oder verschachtelte Aufgaben ausgeführt.

Wenn der Workflow auf Aufgabenebene abgelehnt wird, wird kein Teil der Aufgabe ausgeführt.

Hinweis: Eine Aufgabe, die für die Workflow-Kontrolle auf Aufgabenebene konfiguriert ist, kann gleichzeitig auch für die Workflow-Kontrolle auf Ereignisebene konfiguriert werden. Gleichzeitige Workflows auf Ereignisebene können global oder auf eine bestimmte Aufgabe angewendet werden.

Weitere Informationen

Wokflow auf Ereignisebene (siehe Seite 290)
Globale Prozess-Ereignis-Zuordnung (siehe Seite 312)

Prozessattribut auf Aufgabenebene

Für alle Workflow-Prozesse, die mit einem Workflow auf Aufgabenebene kompatibel sind, ist ein besonderes Attribut im WorkPoint-Designer definiert. Dieses Benutzerdatenattribut auf Prozessebene, TASK_LEVEL, ist in den folgenden Prozessvorlagen standardmäßig auf "wahr" festgelegt:

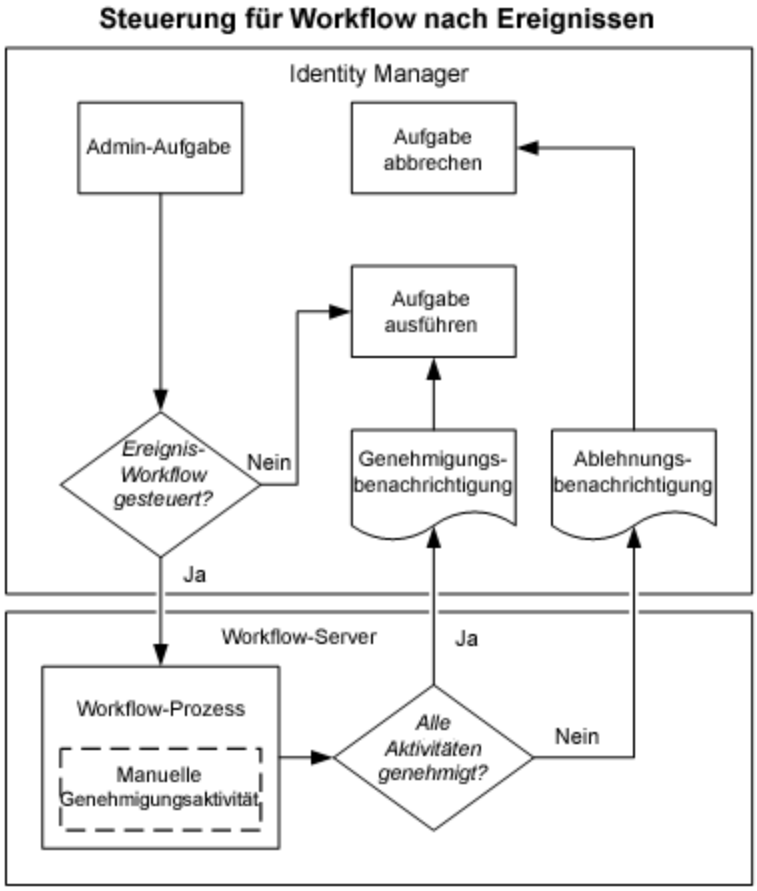
- SingleStepApproval
- TwoStageApprovalProcess
- EscalationApproval

Wenn Sie eine Admin-Aufgabe für den Workflow auf Aufgabenebene auswählen, sind nur diese Prozessvorlagen verfügbar.

Hinweis: Auch wenn TASK_LEVEL auf "wahr" festgelegt ist, können die Prozessvorlagen trotzdem für den Workflow auf Ereignisebene verwendet werden. Ändern Sie diesen TASK_LEVEL-Attributwert nicht.

Kontrolldiagramm auf Aufgabenebene

Im nachstehenden Diagramm ist die Interaktion zwischen CA IdentityMinder und dem Workflow-Server beim Initiieren eines typischen Workflow-Prozesses auf Aufgabenebene dargestellt.



Weitere Informationen:

Kontrolldiagramm auf Ereignisebene (siehe Seite 291)

Konfigurieren des Workflow auf Aufgabenebene - Vorgehensweise

Der Workflow auf Aufgabenebene findet vor der Verarbeitung von Aufgabenaktivitäten statt. Vor Beginn des Workflow-Prozessjobs werden keinerlei Ereignisse oder verschachtelte Aufgaben ausgeführt.

So konfigurieren Sie den Workflow auf Aufgabenebene

1. Wählen Sie in der Benutzerkonsole die Optionen "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe ändern" oder "Admin-Aufgabe erstellen" aus.

   Es wird ein Fenster zur Auswahl der Admin-Aufgabe angezeigt.

2. Suchen Sie die Aufgabe, die Sie der Workflow-Kontrolle unterstellen möchten, und klicken Sie auf "Auswählen".

   Das Fenster "Admin-Aufgabe ändern (oder erstellen)" wird angezeigt.

3. Überprüfen Sie auf der Registerkarte "Profil", ob "Workflow aktivieren" aktiviert ist.

4. Klicken Sie in der Registerkarte "Profil" auf die Schaltfläche "Workflow-Prozess".

   Die Registerkarte für die Workflow-Konfiguration auf Aufgabenebene wird angezeigt.

5. Wählen Sie in der Liste der Workflow-Prozesse eine der folgenden Prozessvorlagen aus:

   - SingleStepApproval
   - TwoStageApprovalProcess

   Die Registerkarte für die Workflow-Konfiguration auf Aufgabenebene wird angezeigt.

6. Konfigurieren Sie Teilnehmer-Resolver, wie dies für die Prozessvorlage erforderlich ist.

   Die Teilnehmeranforderungen werden dem Prozess hinzugefügt.

7. Klicken Sie auf "OK".

   CA IdentityMinder speichert Ihre Workflow-Konfiguration auf Aufgabenebene.

8. Klicken Sie auf "Senden".

   CA IdentityMinder verarbeitet die Aufgabenänderung.

Wokflow auf Ereignisebene

Ein Ereignis kann einem Workflow-Prozess zugeordnet werden. Beim Auslösen eines Ereignisses, das einem Workflow-Prozess zugeordnet ist, wird der Workflow-Prozess gestartet. Die Aufgabe, die das Ereignis auslöste, wird in den Status "Ausstehend" versetzt und der Workflow-Kontrolle unterstellt.

Möglicherweise muss ein Teilnehmer erst ein Ereignis oder eine Aufgabe genehmigen oder ablehnen, bevor ein Workflow-Prozess abgeschlossen werden kann. Eine Aufgabe, für die eine manuelle Workflow-Genehmigung durch einen Teilnehmer erforderlich ist, dauert länger bis zum Abschluss als eine Aufgabe, die nicht der Workflow-Kontrolle unterliegt.

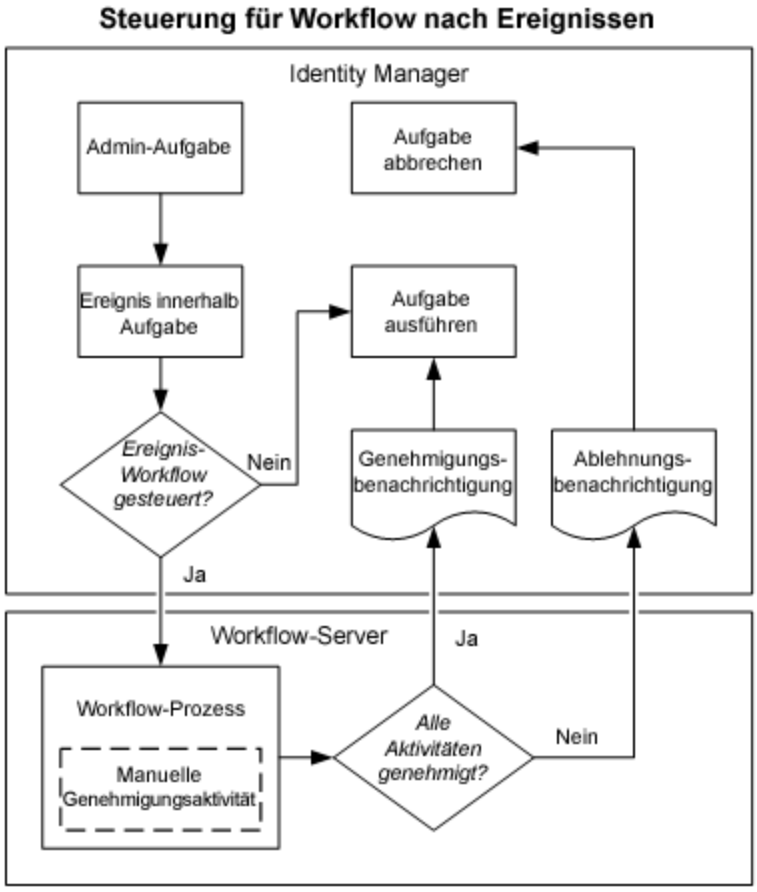
Wenn alle Aktivitäten in einem Workflow-Prozess ausgeführt wurden, wird das dem Workflow-Prozess zugeordnete Ereignis aus der Workflow-Kontrolle freigegeben. Nachdem alle durch eine Aufgabe ausgelösten Ereignisse aus der Workflow-Kontrolle freigegeben wurden, ist die durch den Workflow kontrollierte Aufgabe abgeschlossen.

Während die Aufgabe der Workflow-Kontrolle unterliegt, wird der Fensterinhalt der Aufgaben in der Aufgaben-Persistenz-Datenbank gespeichert. Der Workflow-Jobstatus (Workflow-relevante Daten) wird in der WorkPoint-Datenbank gespeichert.

Hinweis: Die Registerkarte "Ereignisse" listet die Ereignisse auf, die von den Registerkarten in einer Aufgabe generiert werden. Sie müssen die Aufgabe nach dem Hinzufügen einer neuen Registerkarte senden und anschließend mit Hilfe von "Admin-Aufgabe ändern" erneut öffnen, damit die neuen Ereignisse auf der Registerkarte "Ereignisse" angezeigt werden.

Kontrolldiagramm auf Ereignisebene

Im nachstehenden Diagramm ist die Interaktion zwischen CA IdentityMinder und dem Workflow-Server bei der Initiierung eines typischen Workflow-Prozesses auf Ereignisebene dargestellt.



Weitere Informationen:

Kontrolldiagramm auf Aufgabenebene (siehe Seite 288)

Konfigurieren des Workflow auf Ereignisebene - Vorgehensweise

Der Workflow auf Ereignisebene beginnt, wenn ein Ereignis, das einem Workflow-Prozess zugeordnet ist, ausgelöst wird. Die Aufgabe, die das Ereignis ausgelöst hat, wird in den Zustand "In Bearbeitung" versetzt, bis der Teilnehmer die Aufgabe genehmigt oder ablehnt.

So konfigurieren Sie den Workflow auf Ereignisebene:

1. Wählen Sie in der Benutzerkonsole die Optionen "Rollen und Aufgaben", "Admin-Aufgaben" und "Admin-Aufgabe ändern" (oder "Admin-Aufgabe erstellen") aus.

   Es wird ein Fenster zur Auswahl der Admin-Aufgabe angezeigt.

2. Suchen Sie die Aufgabe, die Sie der Workflow-Kontrolle unterstellen möchten, und klicken Sie auf "Auswählen".

   Das Fenster "Admin-Aufgabe ändern (oder erstellen)" wird angezeigt.

3. Überprüfen Sie auf der Registerkarte "Profil", ob "Workflow aktivieren" aktiviert ist.

4. Wählen Sie in der Registerkarte "Ereignisse" ein Ereignis aus, das einer Prozessvorlage zugeordnet werden soll.

   Das Fenster für die Workflow-Zuordnung wird angezeigt.

5. Wählen Sie in der Liste der Workflow-Prozesse eine der folgenden Prozessvorlagen aus:

   - SingleStepApproval
   - TwoStageApprovalProcess

   Das Fenster für die Workflow-Zuordnung wird erweitert.

6. Konfigurieren Sie Teilnehmer-Resolver, wie dies für die Prozessvorlage erforderlich ist.

   Die Teilnehmeranforderungen werden dem Prozess hinzugefügt.

7. Klicken Sie auf "OK".

   CA IdentityMinder speichert Ihre Workflow-Konfiguration auf Ereignisebene.

8. Wiederholen Sie die Schritte 3 - 6 für jedes Ereignis, das Sie der Workflow-Kontrolle unterstellen möchten.

9. Klicken Sie auf "Senden".

   CA IdentityMinder verarbeitet die Aufgabenänderung.

Hinweis: Die Workflow-Prozessliste enthält Prozesse für die Verwendung sowohl mit der Vorlagen- als auch mit der WorkPoint-Methode:

- Bei Auswahl einer Vorlagenmethode (entweder SingleStepApproval oder TwoStageApprovalProcess) wird die Seite erweitert, damit die Teilnehmer-Resolver konfiguriert werden können.
- Bei Auswahl eines Prozesses mit der WorkPoint-Methode wird die Seite nicht erweitert. Teilnehmer-Resolver werden in WorkPoint Designer konfiguriert.

Prozessvorlagentypen

Eine Workflow-Prozessvorlage weist die folgenden Merkmale auf:

- Sie wird in WorkPoint Designer definiert.
- Sie verfügt über manuelle Aktivitäten, die Genehmigungsaufgaben in CA IdentityMinder entsprechen.
- Sie enthält spezielle Attribute, die Informationen zur Identifikation von Teilnehmern (auch Genehmiger genannt) enthält.

Workflow-Prozessvorlagen enthalten keine Informationen für die Auswahl bestimmter Teilnehmer. Diese werden von CA IdentityMinder geliefert, nachdem ein Benutzer einen Workflow und die dazugehörigen Teilnehmer-Resolver konfiguriert hat. Diese Informationen werden einem Ereignis für die Workflow-Kontrolle auf Ereignisebene und einer Aufgabe für die Workflow-Kontrolle auf Aufgabenebene zugeordnet.

Mit der Vorlagenmethode erfolgt die gesamte Workflow- und Teilnehmerkonfiguration in der Benutzerkonsole.

Zur Vorlagenmethode gehören die folgenden drei Prozessvorlagen:

- SingleStepApprovalProcess
- TwoStageApprovalProcess
- EscalationApprovalProcess

Funktionsweise einer Prozessvorlage

Eine Workflow-Prozessvorlage enthält eine Reihe von Orten, an denen Teilnehmerlisten angefordert werden. Wenn die Vorlage einer Aufgabe oder einem Ereignis in CA IdentityMinder zugeordnet wird, müssen Sie Teilnehmer-Resolver für diese Listen konfigurieren.

Zur Laufzeit stellt CA IdentityMinder dem Workflow-Prozess die Teilnehmerlisten basierend auf den von Ihnen konfigurierten Informationen bereit, wie in der nachstehenden Abbildung dargestellt.

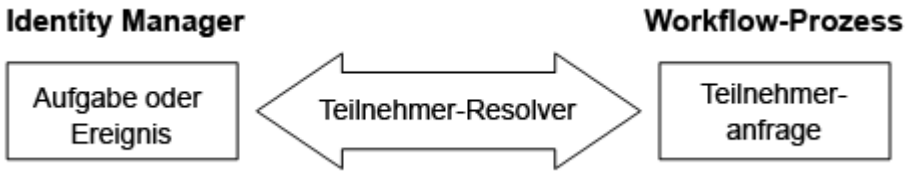


Diagramm einer einstufigen Vorlage

Im nachstehenden Diagramm ist die Prozessvorlage SingleStageApproval so dargestellt, wie sie in WorkPoint Designer erscheint. Die Prozessvorlage enthält zwei manuelle Aktivitäten:

- Einen Genehmigungsknoten für den Hauptteilnehmer. Wenn dieser Benutzer die Anfrage genehmigt oder ablehnt, wird der Prozess bis zum Abschluss ausgeführt.
- Einen Genehmigungsknoten für einen Standard-Teilnehmer. Dieser Benutzer kann die Aufgabe genehmigen oder ablehnen, wenn der Hauptteilnehmer nicht gefunden wird oder nicht antwortet.

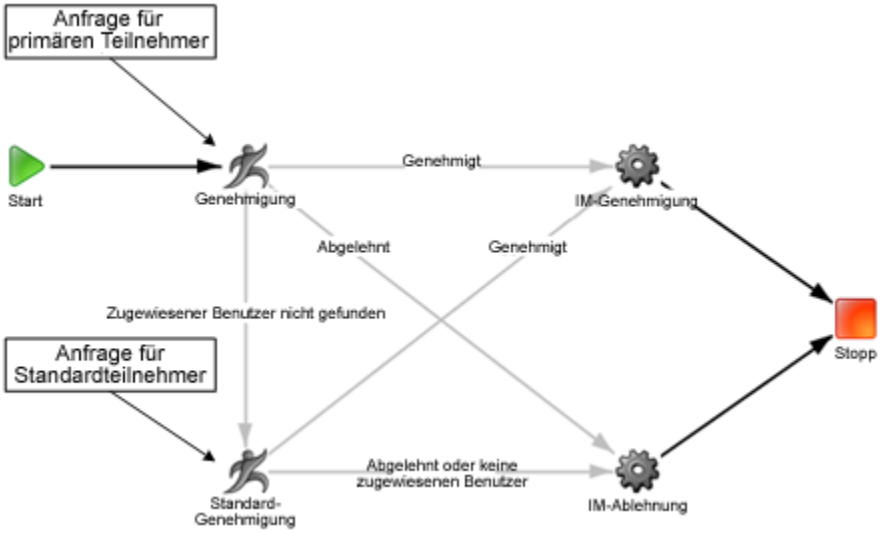


Diagramm einer zweistufigen Vorlage

Im nachstehenden Diagramm ist die Prozessvorlage TwoStageApproval so dargestellt, wie sie in WorkPoint Designer erscheint. Die Prozessvorlage TwoStageApproval enthält drei manuelle Aktivitäten:

- Einen Genehmigungsknoten für den Geschäftsteilnehmer. Wenn dieser Benutzer die Anfrage genehmigt oder ablehnt, wird der Prozess an den technischen Genehmiger weitergeleitet.
- Einen Genehmigungsknoten für den technischen Teilnehmer. Wenn dieser Benutzer die Anfrage genehmigt oder ablehnt, wird der Prozess bis zum Abschluss ausgeführt.
- Einen Genehmigungsknoten für einen Standard-Teilnehmer. Dieser Benutzer kann die Aufgabe genehmigen oder ablehnen, wenn der Geschäfts- oder der technische Teilnehmer nicht gefunden wird oder nicht antwortet.

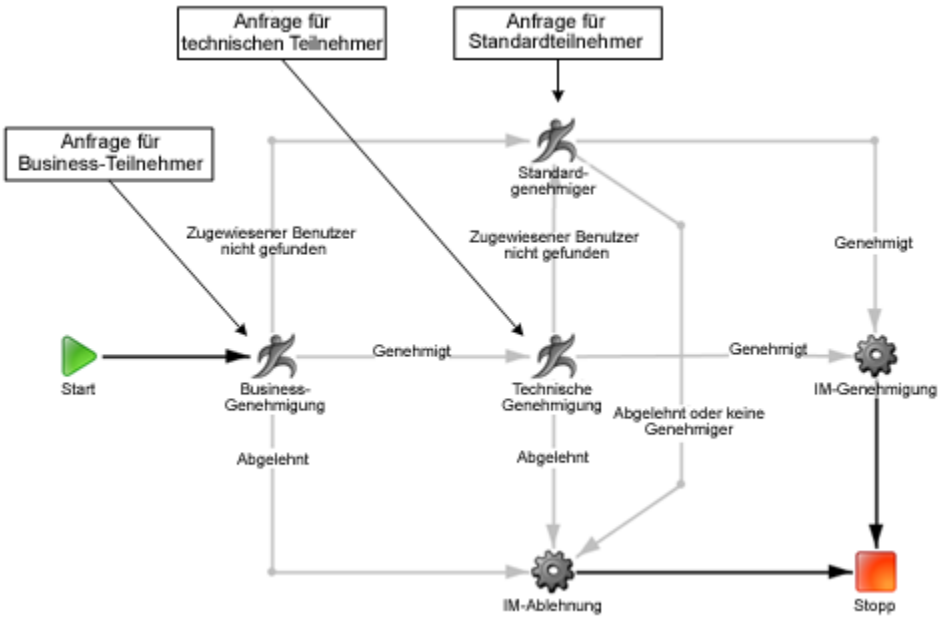
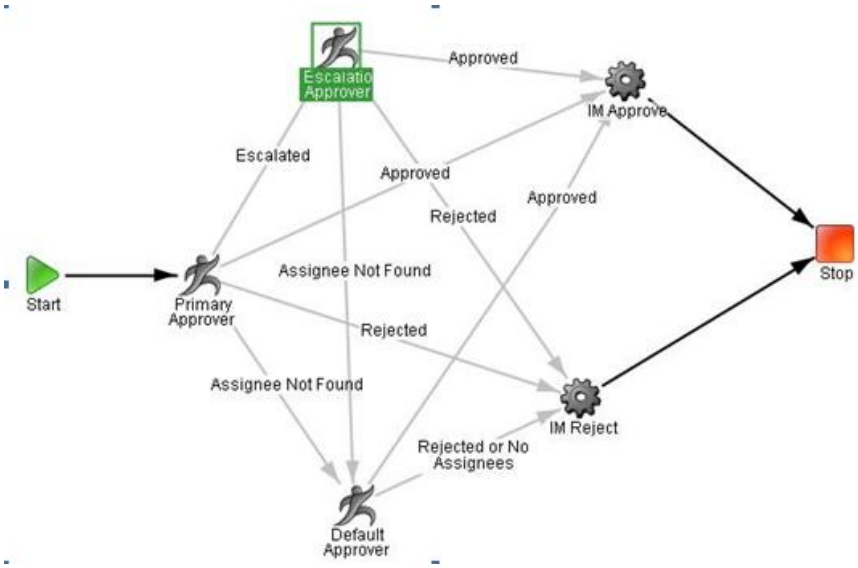


Diagramm der Eskalationsgenehmigungsvorlage

Im nachstehenden Diagramm ist die Prozessvorlage EscalationApproval so dargestellt, wie sie in WorkPoint Designer erscheint. Die Prozessvorlage enthält die folgenden manuellen Aktivitäten:

- Einen Genehmigungsknoten für den Hauptteilnehmer. Wenn dieser Benutzer die Anfrage genehmigt oder ablehnt, wird der Prozess bis zum Abschluss ausgeführt.
- Einen Genehmigungsknoten für einen Standard-Teilnehmer. Dieser Benutzer kann die Anfrage genehmigen oder ablehnen, wenn der Hauptteilnehmer nicht gefunden wird.

- Einen zeitabhängigen Transitionsgenehmigungsknoten vom primären Genehmiger zum Genehmiger der Eskalation. Dieser Benutzer kann die Anfrage genehmigen oder sie ablehnen, wenn der primäre Teilnehmer gefunden wurde, aber nicht im konfigurierten Zeitraum antwortet.



Hinweis: Um die Zeitlimitoption zu einem vorhandenen Prozess hinzuzufügen, fügen Sie das Benutzerdatenfeld PARTICIPANT_TIMEOUT zum Aktivitätsknoten hinzu und fügen Sie "Eskaliert(er)" Übergang zu dem Knoten hinzu, auf dem Sie das Arbeitselement eskaliert haben müssen.

Verwenden der Eskalationsgenehmigungsvorlage

Für die Verwendung der Eskalationsgenehmigungsvorlage müssen Sie die folgende ZIP-Datei manuell importieren, wenn Sie ein Upgrade von r12.5 auf r12.5 SP1 durchführen:

Workflow 12,5 to 12,5 SP1 upgrade.zip

Die ZIP-Datei befindet sich im Ordner "workflowScripts" unter den Verwaltungstools.

. Die Verwaltungstools werden in den folgenden Standardordnern gespeichert:

- Windows: C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
- UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

Arten von Teilnehmer-Resolver

Für die Vorlagenmethode gibt es sieben Arten von Resolver für Teilnehmer:

Rollenmitglieder von Genehmigungsaufgaben

Gibt an, dass Teilnehmer Mitglieder von Rollen sind, die Zugriff auf die Genehmigungsaufgabe gewähren.

Benutzerliste

Gibt an, dass die Teilnehmer eine angegebene Liste von Benutzern darstellen.

Gruppenmitglieder

Gibt an, dass die Teilnehmer Mitglieder einer angegebenen Liste von Gruppen sind.

Mitglieder von Admin-Rollen

Gibt an, dass die Teilnehmer Mitglieder einer angegebenen Liste von Admin-Rollen sind.

Mitglieder von Admin-Aufgaben

Gibt an, dass die Teilnehmer Mitglieder von Admin-Rollen sind, die einer angegebenen Liste von Admin-Aufgaben zugeordnet wurden.

Dynamischer Resolver

Gibt an, dass die Teilnehmer entsprechend der genehmigten Aufgabe bzw. dem genehmigten Ereignis dynamisch ausgewählt werden.

Null-Resolver

Gibt an, dass eine Auflösung zu einer Nullliste ohne Benutzer erfolgt.

Benutzerdefiniert

Gibt die Teilnehmer an, die von einem benutzerdefinierten Teilnehmer-Resolver ermittelt werden.

Rollenmitglieder von Genehmigungsaufgaben

Dieser Resolver weist die Aktivität allen Mitgliedern aller CA IdentityMinder-Rollen zu, die Zugriff auf die Genehmigungsaufgabe gewähren. Für diesen Resolver ist keine weitere Konfiguration erforderlich.

Liste der Benutzer

Diese Auflösung weist das Arbeitselement einer angegebenen Liste von Benutzern zu.

Die Bereichsdefinierung wird nicht durchgesetzt. Jeder Benutzer mit Zugriff auf das Fenster der Workflow-Konfiguration kann einen beliebigen Benutzer zu der Liste hinzufügen oder aus der Liste entfernen.

Diese Auflösung hat die folgenden Validierungsregeln:

- Mindestens ein Benutzername muss angegeben werden.
- Die Benutzernamen müssen zu derzeit vorhandenen Benutzern gehören.

Gruppenmitglieder

Diese Auflösung weist das Arbeitselement allen Mitgliedern aller Gruppen zu, die in der Gruppenliste angegeben sind.

Die Auswertung der Gruppenmitglieder wird während der Erstellung des Arbeitselements ausgeführt - und nicht während der Festlegung der Teilnehmerauflösung.

Die Bereichsdefinierung wird nicht durchgesetzt. Jeder Benutzer mit Zugriff auf das Fenster der Workflow-Konfiguration kann eine beliebige Gruppe zu der Liste hinzufügen oder aus der Liste entfernen.

Diese Auflösung hat die folgenden Validierungsregeln:

- Mindestens eine Gruppe muss angegeben werden.
- Die Gruppennamen müssen zu derzeit vorhandenen Gruppen gehören.

Mitglieder von Admin-Rollen

Diese Auflösung weist das Arbeitselement allen Mitgliedern der in der Liste der Admin-Rollen angegebenen Admin-Rollen zu.

Die Auswertung der Rollenmitglieder wird zu dem Zeitpunkt ausgeführt, zu dem das Arbeitselement erstellt wird - nicht zu dem Zeitpunkt, zu dem die Teilnehmerauflösung festgelegt ist.

Die Bereichsdefinierung wird nicht durchgesetzt. Jede beliebige Rolle kann von jedem Benutzer mit Zugriff auf das Fenster der Workflow-Konfiguration hinzugefügt oder aus der Liste entfernt werden.

Diese Auflösung hat die folgenden Validierungsregeln:

- Mindestens eine Admin-Rolle muss angegeben werden.
- Die Namen der Admin-Rollen müssen die der gegenwärtig vorhandenen Admin-Rollen sein.

Mitglieder von Admin-Aufgaben

Diese Auflösung weist das Arbeitselement allen Mitgliedern aller Admin-Rollen zu, die den Admin-Aufgaben zugeordnet sind, die in der Admin-Aufgaben-Liste angegeben sind.

Die Bereichsdefinierung wird nicht durchgesetzt. Jeder Benutzer mit Zugriff auf das Fenster der Workflow-Konfiguration kann eine beliebige Aufgabe zu der Liste hinzufügen oder aus der Liste entfernen.

Die Auswertung der Rollenmitglieder und davon, welche Rollen in den Aufgaben vorhanden sind, wird während der Erstellung des Arbeitselements ausgeführt - und nicht während der Festlegung der Teilnehmerauflösung.

Diese Auflösung hat die folgenden Validierungsregeln:

- Mindestens eine Admin-Aufgabe muss angegeben werden.
- Die Namen der Admin-Aufgaben müssen die der gegenwärtig vorhandenen Admin-Aufgaben sein.

Dynamischer Resolver

Dieser Resolver gibt eine Liste von Benutzern entsprechend einer dynamischen Regel zurück, die zur Laufzeit aufgelöst wurde. Nehmen Sie zum Einrichten dynamischer Regelbeschränkungen die folgende Auswahl vor:

Genehmiger

Gibt den Typ des Benutzers an, der diese Aufgabe genehmigen soll.

Hinweis: Hiermit werden lediglich die Objekte angezeigt, die Benutzer (oder Genehmiger) enthalten können.

Benutzer oder Objekt

Gibt den Benutzer oder das Objekt an, unter dem die Genehmiger gefunden werden können.

- Diesem Ereignis zugeordnetes Objekt: Das der Workflow-Kontrolle unterstellte Ereignis.
- Initiator dieser Aufgabe: Der Benutzer, der die Admin-Aufgabe initiiert hat.
- Primäres Objekt dieser Aufgabe: Das Objekt, das durch die Aufgabe erstellt oder geändert wird.
- Vorheriger Genehmiger für diese Aufgabe: Die vorherigen Genehmiger dieser Aufgabe.

Benutzer diesem Konto zugewiesen

Aktualisiert das Feld "Benutzer- oder Objektattribut", sodass CA IdentityMinder-Benutzerattribute anstelle von Endpunktkontoattribute angegeben werden. Die Auflösung arbeitet Attribute auf der CA IdentityMinder-Benutzerebene ab. Dieses Kontrollkästchen ist von Bedeutung, wenn Sie ein Endpunktkontoobjekt, wie ein Activ Directory-Konto auswählen.

Attribut

Gibt das Attribut an, das die Genehmiger enthält.

Hinweis: Die Attributliste ist in alphabetischer Reihenfolge sortiert und enthält eine Liste mit eindeutigen Anzeigenamen. Erweiterte Attribute sind aus der Liste ausgeschlossen.

Ereignisobjekttyp

Gibt den Objekttyp des Ereignisses an.

Hinweis: Diese Option wird nur angezeigt, wenn "Diesem Ereignis zugeordnetes Objekt" ausgewählt ist.

Hinweis: Die dynamische Auflösung mit "Gruppe erstellen" erfordert, dass das Objekt vorhanden ist. Informationen bezüglich Gruppenmitgliedschaft/Administratoren können nur mit der dynamisch Auflösung oder der Auflösung der Attributübereinstimmung für vorhandene Gruppen verwendet werden.

Der dynamische Resolver wurde erweitert, um den vorherigen Genehmiger zur Liste der unterstützten Objekte hinzuzufügen. Wenn das physische Attribut ausgewählt wird, das Managerinformationen enthält, routet die Konfiguration die Genehmigung an einen Manager.

So konfigurieren Sie den Resolver als Manager-Genehmigungs-Resolver:

- Legen Sie als Genehmiger "Benutzer" fest.
- Wählen Sie "Vorheriger Genehmiger für diese Aufgabe" aus der Drop-down-Liste "Benutzer oder Objekt" aus.
- Legen Sie als Attribut das physische Attribut fest, das Managerinformationen enthält.

Auflösung der Attributübereinstimmung

Dieser Resolver funktioniert nur für Objekte des Typs "Benutzer". Ein Wert aus einem beliebigen verfügbaren Objekt wird mit einem Feld auf dem Benutzerobjekt verglichen. Nehmen Sie zum Festlegen von Regelbeschränkungen für die Attributübereinstimmung die folgende Auswahl vor:

Genehmiger

Gibt den Typ des Benutzers an, der diese Aufgabe genehmigen soll.

Benutzer oder Objekt

Gibt den Wert an, den Genehmiger im unten ausgewählten Attribut haben.

Hinweis: Der aus dem Benutzer oder Objekt abgerufene Wert sollte ein annehmbarer Wert für eine Suche nach Benutzer für das ausgewählte Attribut sein.

- Diesem Ereignis zugeordnetes Objekt: Das der Workflow-Kontrolle unterstellte Ereignis.
- Initiator dieser Aufgabe: Der Benutzer, der die Admin-Aufgabe initiiert hat.
- Primäres Objekt dieser Aufgabe: Das Objekt, das durch die Aufgabe erstellt oder geändert wird. (Nur für die Ereigniszuordnung auf Aufgabenebene verfügbar.)
- Vorheriger Genehmiger für diese Aufgabe: Die vorherigen Genehmiger dieser Aufgabe.

Benutzer diesem Konto zugewiesen

Aktualisiert das Feld "Benutzer- oder Objektattribut", sodass CA IdentityMinder-Benutzerattribute anstelle von Endpunktkontoattribute angegeben werden. Die Auflösung arbeitet Attribute auf der CA IdentityMinder-Benutzerebene ab. Dieses Kontrollkästchen ist von Bedeutung, wenn Sie ein Endpunktkontoobjekt, wie ein Activ Directory-Konto auswählen.

Benutzer- oder Objektattribut

Gibt das Attribut an, das den in der Suche nach Genehmigern zu verwendenden Wert enthält.

Genehmigersuche - Attribute

Gibt das Attribut an, das in der Suche für die Übereinstimmung mit dem oben angegebenen Wert verwendet wird.

Hinweis: Wenn Sie die Aufgabe "'Benutzer erstellen' genehmigen" auf "Auflösung der Attributübereinstimmung" für Benutzer festlegen (Teilnehmerauflösung), müssen Sie die Methodensignatur für das imApprovers-Skript im WorkPoint-Designer zum Verweis auf den eindeutigen Namen für TwoStageProcessDefinition ändern.

Null-Resolver

Die Null-Auflösung gibt keine Benutzer zurück. Abhängig davon, wie der Workflow-Prozess konzipiert ist, kann dies dazu führen, dass der Prozess die Genehmigung gänzlich überspringt. Die Null-Auflösung erfordert keine weitere Konfiguration.

Benutzerdefinierter Teilnehmer-Resolver

Der benutzerdefinierte Teilnehmer-Resolver ist ein Java-Objekt, das Workflow-Aktivitätsteilnehmer ermittelt und als Liste an CA IdentityMinder zurückgibt. Die Anwendung wiederum leitet die Liste an die Workflow-Engine weiter. Normalerweise erstellen Sie nur dann einen benutzerdefinierten Teilnehmer-Resolver, wenn die Standard-Teilnehmerrichtlinien keine Teilnehmerliste liefern, die für die Aktivität erforderlich sind.

Hinweis: Sie erstellen eine benutzerdefinierte Teilnehmerauflösung mithilfe der Teilnehmerauflösungs-API. Weitere Informationen finden Sie im *Programmierhandbuch für Java*.

Festlegen einer E-Mail-Richtlinie für einen Workflow-Prozess

Sie können eine E-Mail-Richtlinie für jeden Schritt des Workflow-Prozesses angeben. Basierend auf der definierten E-Mail-Richtlinie wird eine E-Mail gesendet, wenn ein Prozess einen entsprechenden Schritt oder eine Aktivität erreicht. Für E-Mail-Benachrichtigungen, die mit einem Workflow-Prozess verknüpft sind, können Sie nur den *Sendezeitpunkt*-Typ *Ausstehende Workflow-E-Mail* auswählen.

Hinweis: Weitere Informationen zu E-Mail-Richtlinien finden Sie unter "How to Create Email Notification Policies".

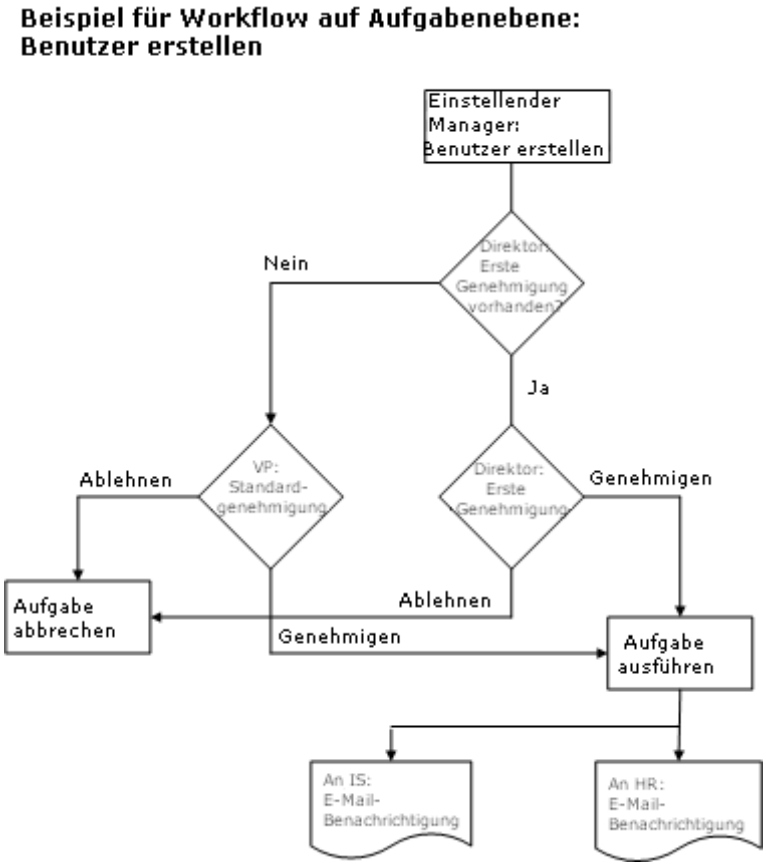
Workflow-Beispiel: Benutzer erstellen

Für die Handhabung folgender Szenarien muss der CA IdentityMinder-Administrator eines Unternehmens einen Workflow und Benutzerrollen definieren:

- Der Vertriebs-Manager der Firma stellt einen neuen Vertriebsmitarbeiter ein. Der Vertriebs-Manager muss in der Lage sein, einen CA IdentityMinder-Benutzer für den neu eingestellten Mitarbeiter zu erstellen.
- Um den Einstellungsprozess zu straffen, möchten die Teilnehmer nur ein einziges Arbeitselement ausführen, um die Aufgabe zu genehmigen (oder abzulehnen).
- Der Vertriebsdirektor sollte der primäre Genehmiger für sämtliche Neueinstellungen sein. Sollte der Vertriebsdirektor aus bestimmten Gründen nicht in der Lage sein, sollte der VP of Sales zum Standardgenehmiger werden.
- Wenn die Neueinstellung genehmigt wurde, soll CA IdentityMinder eine E-Mail-Benachrichtigung über den neuen Benutzer an die Abteilungen Human Resources (HR) und Information Services (IS) senden.

Kontrolldiagramm "Benutzer erstellen"

Das folgende Diagramm zeigt den logischen Ablauf für das Szenario "Benutzer erstellen":



Implementierung des Workflow-Beispiels

Um dieses Beispielszenario zu implementieren, muss der Administrator folgende Aufgaben ausführen:

- Er muss sicherstellen, dass der Aufgabeninitiator ein Mitglied der erforderlichen Admin-Rolle ist.

  Der Vertriebs-Manager muss ein Mitglied der Admin-Rolle "Benutzer-Manager" sein. Diese Rolle gibt dem Vertriebs-Manager die erforderlichen Berechtigungen, um die Admin-Aufgabe "Benutzer erstellen" für den neu eingestellten Vertriebsmitarbeiter zu initiieren.

- Er muss den Workflow auf Aufgabenebene für die Admin-Aufgabe "Benutzer erstellen" aktivieren.

  Der Workflow auf Aufgabenebene gewährleistet, dass nur ein Arbeitselement zum Fertigstellen der Aufgabe "Benutzer erstellen" generiert wird. Da mehrere einzelne Ereignisse mit der Aufgabe "Benutzer erstellen" verknüpft sind, würde ein Workflow auf Ereignisebene verschiedene Arbeitselemente generieren und wäre außerdem schwieriger zu konfigurieren.

- Er muss die Teilnehmer-Resolvers konfigurieren.

  Die Anzahl der möglichen Teilnehmer-Resolver wird durch die ausgewählte Workflow-Prozessvorlage bestimmt. Die Vorlage "SingleStageApproval" umfasst primäre und Standardgenehmiger, andere Vorlagen lassen mehr zu.

  Da dieses Szenario lediglich zwei einzelne Genehmiger erfordert, liefert der Teilnehmer-Resolver "Benutzerliste" die einfachste Lösung. Dieser Resolver ermöglicht die Auswahl individueller Genehmiger per Name, anstelle der Auswahl mehrerer Benutzer pro Rolle oder Gruppe.

- Er muss die E-Mail-Benachrichtigung konfigurieren.

  Die Management-Konsole ermöglicht E-Mail-Benachrichtigungen für bestimmte Aufgaben und Ereignisse. Für dieses Szenario sind Ereignis-E-Mails aktiviert und E-Mail-Benachrichtigungen werden versandt, wenn die Aufgabe "Benutzer erstellen" abgeschlossen wird.

  Eine benutzerdefinierte E-Mail-Vorlage ist erforderlich, um eine E-Mail an die HR- und IS-Abteilungen mit passender Betreffzeile und Nachrichtentext zu senden.

Weitere Informationen:

E-Mail-Benachrichtigungen (siehe Seite 385)
Stellen von Admin-Aufgaben unter Workflow-Kontrolle - Vorlagenmethode (siehe Seite 285)
Konfigurieren des Workflow auf Aufgabenebene - Vorgehensweise (siehe Seite 289)

Verwenden der WorkPoint-Methode

Die bei CA IdentityMinder-Versionen vor r12 verwendete WorkPoint-Methode. Es gibt 14 vordefinierte WorkPoint-Workflow-Prozesse, die standardmäßig bestimmten CA IdentityMinder-Ereignissen zugeordnet sind. Sie müssen WorkPoint Designer verwenden, um die Teilnehmer-Resolver zu konfigurieren und um die Workflow-Prozesse anderweitig zu ändern.

Bei der WorkPoint-Methode müssen Sie auch die Management-Konsole verwenden, um einen Workflow-Prozess einem Genehmigungsereignis zuzuordnen, damit eine entsprechende Aufgabe der Workflow-Kontrolle auf globaler Ebene innerhalb der Umgebung unterstellt werden kann.

In diesem Abschnitt werden die übergeordneten Schritte aufgelistet, die für das Unterstellen von Admin-Aufgaben unter die Workflow-Kontrolle mittels der WorkPoint-Methode nötig sind.

Hinweis: Für mehr Flexibilität und Benutzerfreundlichkeit empfiehlt CA, die Vorlagen-Methode wann immer möglich zu verwenden.

So verwenden Sie die WorkPoint-Methode

1. Konfigurieren Sie Verwaltungstools von WorkPoint. (siehe Seite 306)
2. In der Managementkonsole:
   a. Stellen Sie sicher, dass der Workflow für Ihre Umgebung aktiviert ist, indem Sie das Kontrollkästchen "Aktiviert" unter "Erweiterte Einstellungen", "Workflow" aktivieren.

      Hinweis: Die Ereigniszuordnungen in diesem Fenster gelten nur, wenn Sie den Workflow mit der WorkPoint-Methode konfigurieren. Wenn Sie die Vorlagenmethode (empfohlen) verwenden, ordnen Sie in dieser Management-Konsole Prozessen keine Ereignisse zu.

   b. (Optional) Weisen Sie bei einer globalen Ereigniszuordnung dem entsprechend vordefinierten Workflow-Prozess ein oder mehrere Ereignisse zu.

   c. Starten Sie gegebenenfalls die CA IdentityMinder-Umgebung neu.
3. In der Benutzerkonsole:
   a. Weisen Sie für eine aufgabenspezifische Ereigniszuordnung mindestens ein Ereignis dem passenden vordefinierten Workflow-Prozess zu. (optional)
4. In WorkPoint Designer:
   a. Weisen Sie einer Genehmigungsaufgabe einem Workflow-Prozess zu (optional).

   b. Konfigurieren Sie einen Teilnehmer-Resolver mit einem Workflow-Prozess (optional).
5. In der Benutzerkonsole:
   a. Nachdem die Workflow-Kontrolle konfiguriert wurde, führt der Benutzer mit der entsprechenden Rolle die Admin-Aufgabe aus.

   b. Der vorgesehene Workflow-Teilnehmer genehmigt das Ereignis oder lehnt es ab.

Weitere Informationen:

Ereignissen Prozesse zuordnen (siehe Seite 313)
Zuweisen einer Workflow-Aktivität zu einer Genehmigungsaufgabe (siehe Seite 318)
Teilnehmer-Resolver: WorkPoint-Methode (siehe Seite 319)

Konfigurieren der Verwaltungstools von WorkPoint

WorkPoint Designer ist eine in CA IdentityMinder integrierte Software von Workpoint LLC, einer Tochtergesellschaft von Planet Group, Inc. Mit WorkPoint Designer können Sie Workflow-Prozesse und Workflow-Jobs verwalten. Zu den Verwaltungstools von WorkPoint zählen WorkPoint Designer und WorkPoint Archive. Damit Sie die Verwaltungstools von WorkPoint konfigurieren können, müssen Sie die Verwaltungstools von CA IdentityMinder installieren. Wenn Sie die Verwaltungstools von CA IdentityMinder nicht installiert haben, können Sie das Installationsprogramm ausführen und die Option "CA IdentityMinder Administrative Tools" (<idmgr>-Verwaltungstools) auswählen.

Hinweis: Zur Verwendung der Verwaltungstools im Rahmen des Workflows muss ein unterstütztes JDK auf dem System installiert sein, auf dem auch die Verwaltungstools installiert sind. Eine vollständige Liste der unterstützten Plattformen und Versionen finden Sie in der CA IdentityMinder-Support-Matrix auf der Support-Website von CA IdentityMinder.

Die Workflow-Client-Tools befinden sich im Verzeichnis \WorkPoint in den CA IdentityMinder Verwaltungstools. Die Verwaltungstools werden in den folgenden Standardordnern gespeichert:

- **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

Mit den Tools in diesem Verzeichnis können Sie Folgendes durchführen:

- Workflow-Datenbankschema erstellen
- Standard-Workflow-Skripte laden
- Workflow-Prozesse und -Jobs entwerfen und überwachen

Konfigurieren der Verwaltungstools von WorkPoint auf JBoss

Bearbeiten Sie zum Konfigurieren der Verwaltungstools von WorkPoint auf JBoss die Dateien "init.bat" bzw. "ini.sh" und "workpoint-client.properties".

"init.bat" bzw. "init.sh" bearbeiten

So bearbeiten Sie "init.bat" bzw. "init.sh"

1. Bearbeiten Sie eine der folgenden Dateien in einem Texteditor:
   - **Windows:**

     admin_tools\Workpoint\bin\init.bat
   - **UNIX:**

     *admin_tools/*Workpoint/bin/init.sh
2. Kommentieren Sie die EJB_CLASSPATH-Zeile im JBoss-Abschnitt der Datei aus.

   Hinweis: Stellen Sie sicher, dass alle Abschnitte für andere Anwendungsserver kommentiert sind.
3. Kopieren Sie die Datei jbossall-client.jar von *jboss_home*\client\ nach:

   admin_tools\Workpoint\lib

"workpoint-client.properties" bearbeiten

Bearbeiten Sie die Datei workpoint-client.properties entsprechend dem Typ des von Ihnen im Rahmen der Installation von CA IdentityMinder gewählten Anwendungsservers.

So konfigurieren Sie die Datei "workpoint-client.properties"

1. Öffnen Sie *admin_tools*\Workpoint\conf\ "workpoint-client.properties" in einem Text-Editor.

   admin_tools ist das Installationsverzeichnis der Verwaltungstools. Die Verwaltungstools werden in den folgenden Standardordnern gespeichert:
   - **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools
2. Suchen Sie den Abschnitt JBOSS SETTINGS.

3. Entfernen Sie die Kommentarzeichen vor allen Eigenschaftswerten in diesem Abschnitt.

   Beispiel:

   ```
   java.naming.provider.url=localhost
   java.naming.factory.initial=org.jnp.interfaces.NamingContextFactory
   java.naming.factory.url.pkgs=org.jboss.naming
   ```

   Hinweis: Gegebenenfalls müssen Sie den Wert der Eigenschaft java.naming.provider.url bearbeiten. Ersetzen Sie beispielsweise localhost durch jnp://*Servername oder ip*:*port*. Stellen Sie sicher, dass Sie die jnp-Portnummer 1099 verwenden.

4. Speichern Sie die Datei.

Konfigurieren der Verwaltungstools von WorkPoint auf WebLogic

Bearbeiten Sie zum Konfigurieren der Verwaltungstools von WorkPoint auf WebLogic die Dateien "init.bat" bzw. "ini.sh" und "workpoint-client.properties".

"init.bat" bzw. "init.sh" bearbeiten

So bearbeiten Sie "init.bat" bzw. "init.sh"

1. Bearbeiten Sie eine der folgenden Dateien in einem Texteditor:
   - **Windows:**

     admin_tools\Workpoint\bin\init.bat
   - **UNIX:**

     admin_tools/Workpoint/bin/init.sh
2. Kommentieren Sie EJB_CLASSPATH im WebLogic-Abschnitt der Datei aus:

   Hinweis: Stellen Sie sicher, dass alle Abschnitte für andere Anwendungsserver kommentiert sind.
3. Kopieren Sie die Datei wlclient.jar von *weblogic_home*\server\lib nach:

   admin_tools\Workpoint\lib\

"workpoint-client.properties" bearbeiten

Bearbeiten Sie die Datei workpoint-client.properties entsprechend dem Typ des von Ihnen im Rahmen der Installation von CA IdentityMinder gewählten Anwendungsservers.

So konfigurieren Sie die Datei "workpoint-client.properties"

1. Öffnen Sie *admin_tools*\Workpoint\conf\ "workpoint-client.properties" in einem Text-Editor.
2. Suchen Sie nach dem WebLogic-Abschnitt der Datei.

3. Kommentieren Sie alle Eigenschaftswerte in diesem Abschnitt aus.
4. Speichern Sie die Datei.

   Hinweis: Die Eigenschaft java.naming.provider.url muss auf den voll qualifizierten Domänennamen und die WebLogic-Portnummer des Systems verweisen, auf dem Sie den CA IdentityMinder-Server installiert haben.

Konfigurieren der Verwaltungstools von WorkPoint auf WebSphere

Bearbeiten Sie zum Konfigurieren der Verwaltungstools von WorkPoint auf WebSphere die Dateien "init.bat" bzw. "ini.sh" und "workpoint-client.properties".

"init.bat" bzw. "init.sh" bearbeiten

So bearbeiten Sie "init.bat" bzw. "init.sh"

1. Bearbeiten Sie eine der folgenden Dateien in einem Texteditor:
   - **Windows:**

     admin_tools\Workpoint\bin\init.bat
   - **UNIX:**

     admin_tools/Workpoint/bin/init.sh
2. Kommentieren Sie den IBM WebSphere-Abschnitt aus.

   Hinweis: Fügen Sie kein Kommentarzeichen vor dem Eintrag WP_CLASSPATH im Abschnitt COMMON WP_CLASSPATH ein.
3. Stellen Sie sicher, dass alle Abschnitte für andere Anwendungsserver kommentiert sind.
4. Ersetzen Sie bei Bedarf die Werte für JAVA_HOME und WAS_HOME durch die entsprechenden Pfade für Ihre Umgebung.

"workpoint-client.properties" bearbeiten

Bearbeiten Sie die Datei workpoint-client.properties entsprechend dem Typ des von Ihnen im Rahmen der Installation von CA IdentityMinder gewählten Anwendungsservers.

So konfigurieren Sie die Datei "workpoint-client.properties"

1. Öffnen Sie *admin_tools*\Workpoint\conf\ "workpoint-client.properties" in einem Text-Editor.

   admin_tools ist das Installationsverzeichnis der Verwaltungstools. Die Verwaltungstools werden in den folgenden Standardordnern gespeichert:

   - **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

2. Suchen Sie den Abschnitt IBM WEBSPHERE SETTINGS.
3. Entfernen Sie die Kommentarzeichen vor allen Eigenschaftswerten in diesem Abschnitt.

   Beispiel:
   `java.naming.factory.initial=com.ibm.websphere.naming.WsnInitialContextFactory`
   `java.naming.provider.url=iiop://localhost:`*`bootstrap_port`*

   Hinweis: Die Bootstrap-Portnummer muss der in der WebSphere-Verwaltungskonsole festgelegten Portnummer entsprechen. Die richtige Portnummer finden Sie unter "Server > Endpunkte > Bootstrap server address (Boot-Server-Adresse)".

4. Aktualisieren Sie den BOOTSTRAP_ADDRESS-Port für das WebSphere-Profil wie folgt:
   a. Wechseln Sie in der WebSphere-Verwaltungskonsole zu "Anwendungsserver > Servername > Kommunikationen".
   b. Erweitern Sie die Port-Einträge.
   c. Bearbeiten Sie die Datei workpoint-client.properties unter iam_im.ear/config.
   d. Ändern Sie den Standardport 2809 im Abschnitt "WebSphere" in den Port für BOOTSTRAP_ADDRESS, der im Profil angegeben ist.
5. Speichern Sie die Datei.

Starten von WorkPoint Designer

Führen Sie zum Starten von WorkPoint Designer die folgende Datei aus:

- **Windows:** *admin_tools*\WorkPoint\bin\Designer.bat
- **UNIX:** *admin_tools*/WorkPoint/bin/Designer.sh

Wobei *admin_tools* dem Installationsverzeichnis der CA IdentityMinder Verwaltungstools Die Verwaltungstools werden in den folgenden Standardordnern gespeichert:

- **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

entspricht.

Hinweis: Vor dem Ausführen von WorkPoint Designer müssen Workflow-Komponenten installiert und konfiguriert werden. Weitere Informationen hierzu finden Sie im Abschnitt "Konfigurieren der Verwaltungstools von WorkPoint" zu Ihrem Anwendungsserver.

Weitere Informationen

Konfigurieren der Verwaltungstools von WorkPoint auf JBoss (siehe Seite 306)
Konfigurieren der Verwaltungstools von WorkPoint auf WebLogic (siehe Seite 308)
Konfigurieren der Verwaltungstools von WorkPoint auf WebSphere (siehe Seite 309)

WorkPoint-Prozesse

CA IdentityMinder verfügt über eine Anzahl an Workflow-Prozessen, die im WorkPoint Designer vordefiniert sind. Sie können die vordefinierten Prozesse mit deren Standard-Ereigniszuordnungen verwenden, die Workflow-Prozesse anderen Ereignissen zuordnen, Workflow-Prozesse ändern, indem Sie Aktivitäten hinzufügen oder entfernen, oder neue Workflow-Prozesse erstellen.

Globale Prozess-Ereignis-Zuordnung

Die Zuordnung eines Workflow-Prozesses zu einem Ereignis kann auf der globalen Ebene nicht richtlinienbasiert oder richtlinienbasiert sein.

Weitere Informationen zum Zuordnen eines Ereignisses zu einem Workflow-Prozess mit Hilfe eines richtlinienbasierten Workflow finden Sie unter Globale, richtlinienbasierte Workflow-Zuordnung auf Ereignisebene.

Diese Tabelle zeigt die globalen Standard-Workflow-Prozesse und Ereigniszuordnungen, die in der Management-Konsole spezifiziert sind.

Wichtig: Dies sind globale Zuordnungen. Der zugeordnete Workflow-Prozess wird jedes Mal ausgeführt, wenn das entsprechende Ereignis von einer Aufgabe in der Umgebung generiert wird.

Workflow-Prozess	Zugeordnetes Ereignis
CertifyRoleApproveProcess	CertifyRoleEvent
CreateGroupApproveProcess	CreateGroupEvent
CreateOrganizationApproveProcess	CreateOrganizationEvent
CreateUserApproveProcess	CreateUserEvent
DeleteGroupApproveProcess	DeleteGroupEvent
DeleteOrganizationApproveProcess	DeleteOrganizationEvent
DeleteUserApproveProcess	DeleteUserEvent
ModifyAccessRoleMembershipApproveProcess	AssignAccessRoleEvent RevokeAccessRoleEvent
ModifyAdminRoleMembershipApproveProcess*	
ModifyGroupMembershipApproveProcess*	
ModifyOrganizationApproveProcess	ModifyOrganizationEvent
SelfRegistrationApproveProcess	SelfRegisterUserEvent

Hinweis: Workflow-Prozesse, die mit einem Asterisk (*) markiert sind, sind standardmäßig keinem Ereignis zugeordnet.

Weitere Informationen:

Globales Zuordnen von Prozessen zu Ereignissen (siehe Seite 314)
Einen Workflow-Prozess einem Ereignis in einer bestimmten Aufgabe zuweisen. (siehe Seite 315)

Ereignissen Prozesse zuordnen

Sie erstellen und ändern Workflow-Prozesse im WorkPoint Designer. Wenn Sie einen Workflow-Prozess für CA IdentityMinder erstellen, haben Sie eine bestimmte CA IdentityMinder-Aufgabe im Kopf. Die Ausführung dieser Aufgabe wird vom Workflow-Prozess kontrolliert.

Zusätzlich zum Erstellen des Workflow-Prozesses müssen Sie Folgendes erledigen:

- Identifizieren Sie das Ereignis, das von der CA IdentityMinder-Aufgabe generiert wird, wie unter "Admin-Aufgaben und Ereignisse" beschrieben. Sie können einen Workflow-Prozess für jede CA IdentityMinder-Aufgabe erstellen, die ein Ereignis generiert.
- Ordnen Sie den Workflow-Prozess einem Ereignis zu, indem Sie einen der folgenden Schritte befolgen:
  - Weisen Sie einen Workflow-Prozess einem Ereignis global zu.

    Mit dieser globalen Zuweisung wird der Workflow-Prozess jedes Mal ausgelöst, wenn das Ereignis in der Umgebung generiert wird, unabhängig von der Aufgabe, die das Ereignis generiert.
  - Weisen Sie einen Workflow-Prozess einem Ereignis zu, das von einer bestimmten Aufgabe generiert wurde.

    Mit dieser aufgabenspezifischen Zuweisung wird der Workflow-Prozess nur dann ausgelöst, wenn die spezifische Aufgabe das Ereignis generiert.

  Hinweis: Wenn Sie ein Ereignis einem Workflow-Prozess sowohl global als auch aufgabenspezifisch zuordnen, hat der aufgabenspezifische Workflow-Prozess Vorrang.
- Legen Sie einen Teilnehmer-Resolver für die Workflow-Aktivität in dem Workflow-Prozess fest.
- Weisen Sie einer Workflow-Aktivität eine Genehmigungsaufgabe zu.

Weitere Informationen:

Globales Zuordnen von Prozessen zu Ereignissen (siehe Seite 314)
Einen Workflow-Prozess einem Ereignis in einer bestimmten Aufgabe zuweisen. (siehe Seite 315)
Workflow-Aktivitäten (siehe Seite 317)
Teilnehmer-Resolver: WorkPoint-Methode (siehe Seite 319)

Globales Zuordnen von Prozessen zu Ereignissen

Sie ordnen einen Workflow-Prozess einem Ereignis global zu, so dass der Workflow-Prozess jedes Mal ausgeführt wird, wenn das Ereignis von einer Aufgabe in der Umgebung generiert wird.

So ordnen Sie einen Workflow-Prozess einem Ereignis global zu:

1. Öffnen Sie die Management-Konsole, indem Sie die folgende URL in einen Browser eingeben:

   `http://hostname/iam/immanage`

   Hostname

   Definiert dem voll qualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist. Beispiel: myserver.mycompany.com:port.

2. Klicken Sie auf "Umgebungen" und wählen Sie anschließend den Namen der jeweiligen CA IdentityMinder-Umgebung aus.
3. Klicken Sie auf "Erweiterte Einstellungen" und anschließend auf "Workflow".
4. So ordnen Sie einem Ereignis einen Workflow-Prozess zu:
   a. Wählen Sie ein Ereignis aus dem Listenfeld "Ereignisse" aus.
   b. Wählen Sie einen Workflow-Prozess aus dem Listenfeld "Prozess genehmigen" aus.
   c. Klicken Sie auf "Hinzufügen".
5. Nachdem Sie den Ereignissen Workflow-Prozesse zugeordnet haben, klicken Sie auf "Speichern".
6. Starten Sie die CA IdentityMinder-Umgebung neu, damit die Änderungen wirksam werden.

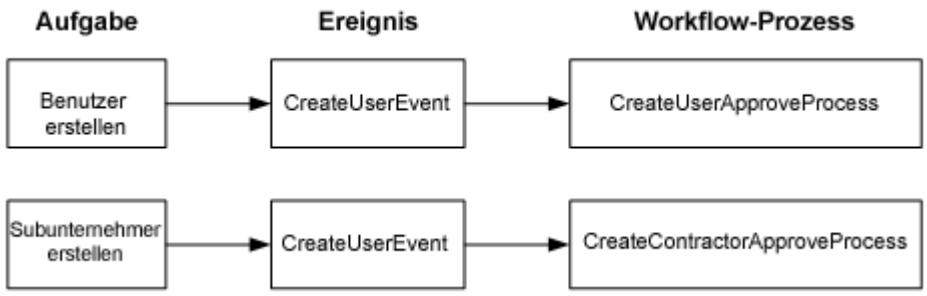
Weitere Informationen:

Globale Prozess-Ereignis-Zuordnung (siehe Seite 312)

Einen Workflow-Prozess einem Ereignis in einer bestimmten Aufgabe zuweisen.

Sie können einen Workflow-Prozess einem Ereignis zuweisen, das von einer bestimmten Aufgabe generiert wurde. In diesem Fall wird der Workflow-Prozess nur dann ausgelöst, wenn das zugeordnete Ereignis von der spezifischen Aufgabe generiert wurde.

Die aufgabenspezifische Zuordnung liefert eine flexible Kontrolle über die Workflow-Prozesse, die für das gleiche Ereignis ausgeführt werden können. Beispiel: Das folgende Diagramm zeigt zwei unterschiedliche Aufgaben, die dasselbe Ereignis generieren, aber zwei unterschiedliche Workflow-Prozesse auslösen:



In diesem Diagramm verwendet jede Aufgabe einen anderen Workflow-Prozess.

Benutzer erstellen

Gibt die Standard-Admin-Aufgabe an, die das Ereignis "CreateUserEvent" auslöst, das dem Standard-Workflow-Prozess "CreateUserApproveProcess" zugeordnet ist.

Auftragnehmer erstellen

Gibt eine benutzerdefinierte Aufgabe an, die auf dem Ereignis "Benutzer erstellen" basiert. In diesem Fall ist das Ereignis "CreateUserEvent" dem benutzerdefinierten Workflow-Prozess "CreateContractorApproveProcess" zugeordnet, der zur Genehmigung von neuen Auftragnehmerkonten erstellt wurde.

So ordnen Sie einen Workflow-Prozess einem Ereignis in einer bestehenden Aufgabe zu:

1. Wählen Sie in der Benutzerkonsole die Optionen "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe ändern" aus.
2. Suchen Sie nach einer Admin-Aufgabe.
3. Wählen Sie eine Aufgabe (z. B. "Benutzer ändern" oder "Benutzer erstellen") aus, und klicken Sie auf "Auswählen".
4. Wählen Sie auf der Registerkarte "Ereignisse" einen Workflow-Prozess für das Ereignis in der Aufgabe aus.

   Hinweis: Die Option "Workflow" muss für die Ereignisnamen aktiviert sein und das Dropdown-Menü "Workflow-Prozess" muss auf der Registerkarte angezeigt werden.

5. Weisen Sie über das Dropdown-Menü "Workflow-Prozess" einen Workflow-Prozess dem Ereignisnamen zu und klicken Sie auf "OK".
6. Klicken Sie auf "Senden".
7. Öffnen Sie die Management-Konsole und starten Sie die CA IdentityMinder-Umgebung neu, damit die Änderungen wirksam werden.

So ordnen Sie einen Workflow-Prozess einem Ereignis in einer neuen Aufgabe zu:

1. Wählen Sie in der Benutzerkonsole "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe erstellen" aus.

   Hinweis: Stellen Sie sicher, dass Sie eine bestehende Workflow-Genehmigungsaufgabe (wie etwa "'Gruppe erstellen' genehmigen" oder "'Benutzer erstellen' genehmigen") als Vorlage für Ihre neue Workflow-Genehmigungsaufgabe auswählen.
2. Geben Sie auf der Registerkarte "Profil" die Informationen in die entsprechenden Felder ein.
3. Wählen Sie auf der Registerkarte "Ereignisse" einen Workflow-Prozess für das Ereignis in der Aufgabe aus.

   Hinweis: Die Option "Workflow" muss für die Ereignisnamen aktiviert sein und das Dropdown-Menü "Workflow-Prozess" muss auf der Registerkarte angezeigt werden.
4. Weisen Sie über das Dropdown-Menü "Workflow-Prozess" einen Workflow-Prozess dem Ereignisnamen zu und klicken Sie auf "OK".
5. Klicken Sie auf "Senden".
6. Öffnen Sie die Management-Konsole und starten Sie die CA IdentityMinder-Umgebung neu, damit die Änderungen wirksam werden.

Hinweis: Die Workflow-Prozessliste enthält Prozesse für die Verwendung sowohl mit der Vorlagen- als auch mit der WorkPoint-Methode:

- Bei Auswahl einer Vorlagenmethode (entweder SingleStepApproval oder TwoStageApprovalProcess) wird die Seite erweitert, damit die Teilnehmer-Resolver konfiguriert werden können.
- Bei Auswahl eines Prozesses mit der WorkPoint-Methode wird die Seite nicht erweitert. Teilnehmer-Resolver werden in WorkPoint Designer konfiguriert.

Weitere Informationen:

Globale Prozess-Ereignis-Zuordnung (siehe Seite 312)

Workflow-Aktivitäten

CA IdentityMinder umfasst eine Anzahl an Workflow-Aktivitäten, die im WorkPoint Designer vordefiniert sind. Diese Aktivitäten werden vordefinierten Workflow-Prozessen zugewiesen.

Die vordefinierten Workflow-Prozesse sind Einzelschrittprozesse, das heißt, jeder Prozess enthält eine einzelne vordefinierte Aktivität.

Jede vordefinierte Aktivität entspricht einer in CA IdentityMinder vordefinierten Workflow-Genehmigungsaufgabe mit demselben Namen. Sie können die vordefinierte Aktivitäten in anderen Workflow-Prozessen verwenden und Sie können neue Aktivitäten erstellen.

Sie können die vordefinierten Workflow-Prozesse unverändert verwenden und brauchen auch keine zusätzlichen Aktivitäten hinzufügen. Weitere Informationen zum Hinzufügen von Aktivitäten zu einem Workflow-Prozess finden Sie in der WorkPoint-Dokumentation.

Prozesse, Aufgaben und Aktivitäten

Die Tabelle unten zeigt die vordefinierten Workflow-Aktivitäten und den vordefinierten Workflow-Prozess, die jeder Aktivität standardmäßig zugewiesen sind.

Hinweis: Die vordefinierten Workflow-Aktivitäten und ihre zugehörigen Workflow-Genehmigungsaufgaben haben denselben Namen.

Workflow-Prozess	Workflow-Aufgabe/-Aktivität
CertifyRoleApprovalProcess**	"Rolle zertifizieren" genehmigen
Beratungsprozess*	
CreateGroupApproveProcess	"Gruppe erstellen" genehmigen
CreateOrganizationApproveProcess	"Organisation erstellen" genehmigen
CreateUserApproveProcess	"Benutzer erstellen" genehmigen
DeleteGroupApproveProcess	"Gruppenprofil löschen" genehmigen
DeleteOrganizationApproveProcess	"Organisationsprofil löschen" genehmigen
DeleteUserApproveProcess	"Benutzerprofil löschen" genehmigen
ModifyAccessRoleMembershipApproveProcess	"Zugriffsrollenmitgliedschaft ändern" genehmigen
ModifyAdminRoleMembershipApproveProcess	"Admin-Rollen-Mitgliedschaft ändern" genehmigen

Workflow-Prozess	Workflow-Aufgabe/-Aktivität
ModifyGroupMembershipApproveProcess	"Gruppenmitgliedschaft ändern" genehmigen
ModifyIdentityPolicySetApproveProcess	"Identitätsrichtliniensatz ändern" genehmigen
ModifyOrganizationApproveProcess	"Organisation ändern" genehmigen
ModifyUserApproveProcess	"Benutzer ändern" genehmigen
SelfRegistrationApproveProcess	Selbstregistrierung genehmigen
SingleStepApproval*	
TwoStageApprovalProcess*	

Hinweis: Workflow-Prozesse, die mit einem Asterisk (*) markiert sind, sind für die Verwendung mit der Vorlagen-Methode konzipiert. Sie werden in der Benutzerkonsole konfiguriert und haben daher keine standardmäßig zugewiesenen Aufgaben oder Aktivitäten. Der Prozess "CertifyRoleApprovalProcess" (**) ist ein Beispielprozess für einen benutzerdefinierten Teilnehmer-Resolver.

Zuweisen einer Workflow-Aktivität zu einer Genehmigungsaufgabe

Um einer Workflow-Aktivität eine Workflow-Genehmigungsaufgabe zuzuweisen, definieren Sie im WorkPoint Designer ein Namen-Werte-Paar.

Hinweis: Falls standardmäßig kein Namen-Wert-Paar für eine Workflow-Aktivität definiert ist, verwendet CA IdentityMinder eine Aufgabe, deren Name mit der Genehmigungsaufgabe übereinstimmt.

So weisen Sie einer Workflow-Aktivität eine bestimmte Genehmigungsaufgabe zu:

1. Starten Sie den WorkPoint Designer.
2. Klicken Sie auf "Datei", "Öffnen" und dann auf "Prozess".
3. Wählen Sie einen Workflow-Prozess aus, und klicken Sie auf "Öffnen".
4. Klicken Sie mit der rechten Maustaste auf den Aktivitätsknoten im Prozess und wählen Sie "Eigenschaften" aus.
5. Wählen Sie im Dropdown-Menü "Typ" die Option "Text" aus.
6. Geben Sie in der Registerkarte "Benutzerdaten" Folgendes ein:
   - **Name**: TASK_TAG.
   - **Wert**: Tag-Name der Genehmigungsaufgabe.
7. Klicken Sie auf "Hinzufügen".
8. Klicken Sie auf "OK", um die Änderungen zu speichern.

Erstellen von Genehmigungsaufgaben für Endpunkte

Sie können Genehmigungsaufgaben für Kontoverwaltungsfenster erstellen. Für Aufgaben, die Kontoänderungen genehmigen, muss das Genehmigungsfenster für einen Endpunkttyp spezifisch sein, so dass der Genehmiger die geänderten Werte sehen kann. Um eine Genehmigungsaufgabe für eine Erstellungs- oder Änderungsaufgabe zu erstellen, gehen Sie wie folgt vor:

So erstellen Sie eine Genehmigungsaufgabe für einen Endpunkt:

1. Klicken Sie in der Benutzerkonsole auf "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe erstellen".
2. Wählen Sie "Kopie einer Admin-Aufgabe erstellen" zum Verwalten von Konten am Endpunkt aus.

   Der Name enthält "erstellen" und gibt den Namen des Endpunkttyps an. Beispiel: Active Directory-Konto erstellen.
3. Nehmen Sie auf der Registerkarte "Profil" die folgenden Änderungen vor.
   - Ändern Sie den Namen der neuen Aufgabe.
   - Ändern Sie den Aufgaben-Tag.
   - Ändern Sie die Aktion in "Ereignis genehmigen".
4. Nehmen Sie auf der Registerkarte "Registerkarten" die folgenden Änderungen vor:
   a. Entfernen Sie alle Beziehungs-Registerkarten.
   b. Kopieren und bearbeiten Sie dann die Genehmigungsfenster auf den Registerkarten nach Bedarf.

      Hinweis: Es können Probleme auftreten, wenn Fenster in einer Genehmigungsaufgabe verwendet werden und Änderungen am Standardkontofenster vorgenommen werden müssen, damit sie in einer Genehmigungsaufgabe funktionieren.
5. Klicken Sie auf "Senden".

Teilnehmer-Resolver: WorkPoint-Methode

Wenn Sie Teilnehmer mit Hilfe der WorkPoint-Methode festlegen möchten, definieren Sie im WorkPoint Designer folgende Aktivitätseigenschaften:

- Den Namen des vordefinierten CA IdentityMinder-Skripts, das die Kommunikation zwischen CA IdentityMinder und dem Workflow-Server ermöglicht. Das Skript sendet eine Anfrage nach Aktivitäts-Teilnehmern an CA IdentityMinder und übermittelt die Liste an den Workflow-Server.
- Verweise zu mindestens einem Teilnehmer-Resolver.

Arten von Teilnehmer-Resolver

Anstatt eine bestimmte Liste mit Teilnehmern bei den Workflow-Aktivitätseigenschaften einzugeben, wird auf die Teilnehmer mit einem frei wählbaren Namen verwiesen, der einem *Teilnehmer-Resolver* zugeordnet ist.

Für das vordefinierte Prozessmodell gibt es vier Arten von Teilnehmer-Resolver:

Teilnehmer-Resolver "Rolle"

Gibt die Teilnehmer an, die Mitglieder einer bestimmten Rolle sind.

Teilnehmer-Resolver "Gruppe"

Gibt die Teilnehmer an, die Mitglieder einer bestimmten Gruppe sind.

Benutzerdefinierter Teilnehmer-Resolver

Gibt die Teilnehmer an, die von einem benutzerdefinierten Teilnehmer-Resolver ermittelt werden.

Teilnehmer-Resolver "Filter"

Gibt die Teilnehmer an, die über einen Suchfilter ausgewählt werden.

Teilnehmer-Resolver "Rolle"

Mit dem Teilnehmer-Resolver "Rolle" ermittelt CA IdentityMinder alle Mitglieder der Rolle und gibt die Mitglieder als Teilnehmer zurück.

Wenn beim Parameter "Benutzerdaten" im Dialogfeld "Aktivität" keine Resolver-Art angegeben ist, wird standardmäßig die Resolver-Art "Rolle" verwendet.

Wenn Sie auf der Registerkarte "Benutzerdaten" des WorkPoint-Dialogfeldes "Aktivitätseigenschaften" keinen Teilnehmer-Resolver festlegen, findet CA IdentityMinder standardmäßig alle verfügbaren Rollen, die diese Genehmigungsaufgabe enthalten, und gibt die Mitglieder jener Rollen als Teilnehmer zurück.

So konfiguieren Sie Teilnehmer-Resolver des Typs "Rolle":

1. Starten Sie den WorkPoint Designer.
2. Klicken Sie auf "Datei", "Öffnen" und dann auf "Prozess".
3. Wählen Sie einen Workflow-Prozess aus, und klicken Sie auf "Öffnen".
4. Klicken Sie mit der rechten Maustaste auf den Aktivitätsknoten im Prozess und wählen Sie "Eigenschaften" aus.
5. Wählen Sie im Dropdown-Menü "Typ" die Option "Text" aus.

6. Geben Sie in der Registerkarte "Benutzerdaten" Folgendes ein:
   - **Name**: APPROVER_ROLE_NAME
   - **Wert** - Der Name einer CA IdentityMinder-Rolle (zum Beispiel "Sicherheits-Manager")
7. Klicken Sie auf "Hinzufügen".

   Hinweis: Diese Rolle muss keine Genehmigungsaufgabe enthalten.
8. Wählen Sie im Dropdown-Menü "Typ" die Option "Text" aus.
9. Geben Sie auf der Registerkarte "Benutzerdaten" folgendes Namen-Werte-Paar ein (optional):

   Name: APPROVERS_REQUIRED

   Wert: YES.
10. Klicken Sie auf "Hinzufügen".

    Hinweis: Die Standard-Genehmigungseinstellung ist APPROVERS_REQUIRED=NO. In diesem Fall wird eine Aktivität automatisch genehmigt, wenn keine Teilnehmer gefunden werden.

    Wenn die Einstellung mit APPROVERS_REQUIRED=YES festgelegt ist und CA IdentityMinder keine Teilnehmer finden kann, wird die Aktivität nicht erfolgreich abgeschlossen.
11. Klicken Sie auf "OK", um die Änderungen zu speichern.

Teilnehmer-Resolver "Gruppe"

Mit dem Teilnehmer-Resolver "Gruppe" ermittelt CA IdentityMinder alle Mitglieder der Gruppe und gibt die Mitglieder als Teilnehmer zurück.

So konfiguieren Sie Teilnehmer-Resolver des Typs "Gruppe":

1. Starten Sie den WorkPoint Designer.
2. Klicken Sie auf "Datei", "Öffnen" und dann auf "Prozess".
3. Wählen Sie einen Workflow-Prozess aus, und klicken Sie auf "Öffnen".
4. Klicken Sie mit der rechten Maustaste auf den Aktivitätsknoten im Prozess und wählen Sie "Eigenschaften" aus.
5. Wählen Sie im Dropdown-Menü "Typ" die Option "Text" aus.
6. Geben Sie in der Registerkarte "Benutzerdaten" Folgendes ein:
   - **Name**: APPROVER_GROUP_UNIQUENAME
   - **Wert** - Der Name einer CA IdentityMinder-Gruppe
7. Klicken Sie auf "Hinzufügen".
8. Wählen Sie im Dropdown-Menü "Typ" die Option "Text" aus.

9. Geben Sie auf der Registerkarte "Benutzerdaten" folgendes Namen-Werte-Paar ein (optional):
   - **Name**: APPROVERS_REQUIRED
   - **Wert**: YES.
10. Klicken Sie auf "Hinzufügen".

    Hinweis: Die Standard-Genehmigungseinstellung ist APPROVERS_REQUIRED=NO. In diesem Fall wird eine Aktivität automatisch genehmigt, wenn keine Teilnehmer gefunden werden.

    Wenn die Einstellung mit APPROVERS_REQUIRED=YES festgelegt ist und CA IdentityMinder keine Teilnehmer finden kann, wird die Aktivität nicht erfolgreich abgeschlossen.
11. Klicken Sie auf "OK", um die Änderungen zu speichern.

Benutzerdefinierter Teilnehmer-Resolver

Der benutzerdefinierte Teilnehmer-Resolver ist ein Java-Objekt, das Workflow-Aktivitätsteilnehmer ermittelt und als Liste an CA IdentityMinder zurückgibt. Die Anwendung wiederum leitet die Liste an die Workflow-Engine weiter. Normalerweise erstellen Sie nur dann einen benutzerdefinierten Teilnehmer-Resolver, wenn die Standard-Teilnehmerrichtlinien keine Teilnehmerliste liefern, die für die Aktivität erforderlich sind.

Hinweis: Sie erstellen einen benutzerdefinierten Teilnehmer-Resolver mit Hilfe der Teilnehmer-Resolver-API. Weitere Informationen finden Sie im *Programmierhandbuch für Java*.

So konfigurieren Sie einen benutzerdefinierten Teilnehmer-Resolver:

1. Öffnen Sie die Management-Konsole, indem Sie die folgende URL in einen Browser eingeben:

   `http://hostname/iam/immanage`

   Hostname

   Definiert dem voll qualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist. Beispiel: myserver.mycompany.com:port.
2. Klicken Sie auf "Umgebungen" und wählen Sie anschließend den Namen der jeweiligen CA IdentityMinder-Umgebung aus.
3. Klicken Sie auf "Erweiterte Einstellungen" und anschließend auf "Workflow-Teilnehmer-Resolver".

4. Klicken Sie auf dem Bildschirm "Workflow-Teilnehmer-Resolver" auf "Neu", und geben Sie anschließend Folgendes ein:

   Name

   Gibt den Namen des benutzerdefinierten Teilnehmer-Resolvers an, z. B. APPROVER_CUSTOMRESOLVER_NAME

   Beschreibung

   Gibt eine Beschreibung des benutzerdefinierten Teilnehmer-Resolvers an.

   Klasse

   Gibt den Namen der Java-Klasse an, z. B. com.netegrity.samples.GroupFinder

5. Klicken Sie auf "Speichern".
6. Starten Sie den WorkPoint Designer.
7. Klicken Sie auf "Datei", "Öffnen" und dann auf "Prozess".
8. Wählen Sie einen Workflow-Prozess aus, und klicken Sie auf "Öffnen".
9. Klicken Sie mit der rechten Maustaste auf den Aktivitätsknoten im Prozess und wählen Sie "Eigenschaften" aus.
10. Wählen Sie im Dropdown-Menü "Typ" die Option "Text" aus.
11. Geben Sie in der Registerkarte "Benutzerdaten" Folgendes ein:

    Name

    Gibt den Namen des benutzerdefinierten Teilnehmer-Resolvers an. Dieser muss dem Namen entsprechen, den Sie im Bildschirm "Benutzerdefinierter Teilnehmer-Resolver" in der CA IdentityMinder-Management-Konsole eingegeben haben, zum Beispiel:

    APPROVER_CUSTOMRESOLVER_NAME

    Wert

    Gibt einen eindeutigen Namen für den benutzerdefinierten Teilnehmer-Resolver an, z. B. GroupFinder.

12. Klicken Sie auf "Hinzufügen".

    Hinweis: Die Standard-Genehmigungseinstellung ist APPROVERS_REQUIRED=NO. In diesem Fall wird eine Aktivität automatisch genehmigt, wenn keine Teilnehmer gefunden werden.

    Wenn die Einstellung mit APPROVERS_REQUIRED=YES festgelegt ist und CA IdentityMinder keine Teilnehmer finden kann, wird die Aktivität nicht erfolgreich abgeschlossen.

13. Klicken Sie auf "OK", um die Änderungen zu speichern.

Teilnehmer-Resolver "Filter"

Mit einem Teilnehmer-Resolver des Typs "Filter" kann CA IdentityMinder nach Benutzern oder Gruppen suchen, die die Filterkriterien erfüllen. Sie definieren im WorkPoint Designer einen Suchfilter und CA IdentityMinder gibt passende Genehmiger für die entsprechende Workflow-Aktivität zurück.

Sie erstellen einen Teilnehmer-Resolver des Typs "Filter" in der Registerkarte "Benutzerdaten" des Dialogfeldes "Aktivitätseigenschaften" von WorkPoint.

Filter-Syntax der Teilnehmer-Resolver

Die folgenden drei Attribute werden zum Definieren eines Suchfilters kombiniert:

- Genehmiger-Attribut, beispielsweise "Titel"
- Genehmiger-Attributvorgang, beispielsweise "gleich"
- Genehmiger-Attributwert, beispielsweise "Manager"

Die erforderlichen Suchfilterattribute werden in folgender Reihenfolge miteinander kombiniert:

Attribut Vorgang Wert

Beispiel:

Titel gleich Manager oder *Abteilung enthält Lohnbuchhaltung*

Erforderliche Filterattribute für Teilnehmer-Resolver

Die *erforderlichen* Filterattribute für Teilnehmer-Resolver sind wie folgt:

Hinweis: Für jeden Filter ist "n" eine positive natürliche Zahl, die die Suchfilternummer angibt. Der Standardwert lautet "1".

APPROVER_FILTER_n_ATTRIBUTE

Gibt das Genehmiger-Attribut an. Beispiel: Titel, Abteilung, Benutzer-ID. (Die Namenszeichenfolgen von Genehmiger-Attributen müssen mit den Namenszeichenfolgen von Benutzer-Attributen aus CA IdentityMinder übereinstimmen.)

APPROVER_FILTER_n_OP

Gibt den mit dem Genehmiger-Attribut verknüpften Operator an. Beispiele: EQUALS, NOT_EQUALS, CONTAINS. (Bei Operatoren spielt die Groß-/Kleinschreibung keine Rolle.)

Gültige Einträge für diesen Filter sind wie folgt:

- EQUALS
- STARTSWITH
- NOT_EQUALS
- CONTAINS
- ENDS_WITH
- GREATER_THAN
- LESS_THAN
- GREATER_THAN_EQUALS
- LESS_THAN_EQUALS

APPROVER_FILTER_n_VALUE

Gibt den mit dem Genehmiger-Attribut verknüpften Wert an. Beispiele: Manager, Lohnbuchhaltung, Engineering.

Optionale Filterattribute für Teilnehmer-Resolver

Die *optionalen* Filterattribute für Teilnehmer-Resolver sind wie folgt:

APPROVER_OBJECTTYPE

USER oder GROUP (unabh. von Groß-/Kleinschreibung)

Der Standardwert ist: USER.

APPROVER_ORG_UNIQUENAME

Ein eindeutiger Organisationsname des Genehmigers. (Die Namenszeichenfolge des Organisationsnamens muss mit der in Identity Manager übereinstimmen.)

Standardmäßig ist dies "root".

APPROVER_ORG_AND_LOWER

Die Organisation oder Unterorganisation des Genehmigers:

- 0 bedeutet: in der Organisation des Genehmigers suchen.
- 1 bedeutet: in allen Unterorganisationen der Organisation des Genehmigers suchen.

Der Standardwert lautet "1".

APPROVER_FILTER_NO

Die Anzahl der Suchfilter, die Sie verwenden. Wenn Sie zwei Filter verwenden, steht die Anzahl auf 2.

Der Standardwert lautet "1".

Hinweis: Dieser Filter ist erforderlich, wenn Sie mehrere Filter verwenden.

APPROVER_FILTER_n_CONJ_TYPE

Sie können Suchfilter über die Operatoren OR und AND miteinander kombinieren.

Hinweis: Filter, die mit dem Operator OR kombiniert werden, haben Vorrang vor solchen, die durch AND getrennt werden.

Sie können zum Beispiel den Operator AND verwenden, wenn Sie nach "Titel EQUALS Manager" AND "Abteilung EQUALS Entwicklung" suchen möchten.

Hinweis: "n" ist eine positive Ganzzahl größer als Eins, die die Suchfilternummer angibt.

Filter des Teilnehmer-Resolver hinzufügen

So fügen Sie einen Filter für Teilnehmer-Resolver hinzu:

1. Starten Sie den WorkPoint Designer.
2. Klicken Sie auf "Datei", "Öffnen" und dann auf "Prozess".
3. Wählen Sie einen Workflow-Prozess aus, und klicken Sie auf "Öffnen".
4. Klicken Sie mit der rechten Maustaste auf den Aktivitätsknoten im Prozess und wählen Sie "Eigenschaften" aus.
5. Wählen Sie im Dropdown-Menü "Typ" die Option "Text" aus.
6. Geben Sie in der Registerkarte "Benutzerdaten" Folgendes ein:
   - **Name**: APPROVER_FILTER_1_ATTRIBUTE
   - **Wert**: Eine eindeutige Rollenidentifikation (Beispiel: Titel).
7. Klicken Sie auf "Hinzufügen".
8. Wiederholen Sie die Schritte 6 und 7 für jedes Attribut im Suchfilter.

   Hinweis: Die Standard-Genehmigungseinstellung ist APPROVERS_REQUIRED=NO. In diesem Fall wird eine Aktivität automatisch genehmigt, wenn keine Teilnehmer gefunden werden.

   Wenn die Einstellung mit APPROVERS_REQUIRED=YES festgelegt ist und CA IdentityMinder keine Teilnehmer finden kann, wird die Aktivität nicht erfolgreich abgeschlossen.
9. Klicken Sie auf "OK", um die Änderungen zu speichern.

Beispiel: Teilnehmer-Resolver "Filter"

Der Benutzerspeicher in der folgenden Tabelle enthält vier Benutzer: Holly, Sarah, John und Dave, jeweils mit Benutzer-ID, Berufsbezeichnung und Abteilungsattributen.

Benutzer	ID	Titel	Abteilung
Holly	admin1	sysadmin	Administration

Benutzer	ID	Titel	Abteilung
Sarah	test1	sysadmin	Entwicklung
John	admin2	Manager	Entwicklung
Dave	admin3	sysadmin	Accounting

CA IdentityMinder wendet die drei Filter, die in der folgenden Tabelle definiert sind, auf den obigen Benutzerspeicher an:

Name	Wert
APPROVER_FILTER_NO	3
APPROVER_FILTER_1_ATTRIBUTE	uid
APPROVER_FILTER_1_OP	EQUALS
APPROVER_FILTER_1_VALUE	admin*
APPROVER_FILTER_2_CONJ_TYPE	AND
APPROVER_FILTER_2_ATTRIBUTE	department
APPROVER_FILTER_2_OP	EQUALS
APPROVER_FILTER_2_VALUE	Administration
APPROVER_FILTER_3_CONJ_TYPE	OR
APPROVER_FILTER_3_ATTRIBUTE	title
APPROVER_FILTER_3_OP	EQUALS
APPROVER_FILTER_3_VALUE	sysadmin

CA IdentityMinder wendet die Filter in folgender Reihenfolge an:

1. Er berechnet den zweiten und den dritten Filter, die mit dem Operator OR verknüpft sind:

   "Abteilung EQUALS Administration" OR "Title EQUALS sysadmin"

   Hierbei wird John ausgeschlossen und Holly, Sarah und Dave werden zurückgegeben.

2. Er berechnet den ersten und den zweiten Filter, die mit dem Operator AND verknüpft sind (wobei * ein Platzhalterzeichen ist):

   "uid EQUALS admin*" AND "Abteilung EQUALS Administration"

   Hierbei wird Sarah ausgeschlossen und Holly und Dave werden zurückgegeben.

Die letztlich vom Benutzerspeicher zurückgegebenen Benutzer sind Holly und Dave.

Rangordnung der Teilnehmer-Resolver

Wenn Sie keinen Teilnehmer-Resolver auswählen, identifiziert Identity Manager standardmäßig alle verfügbaren Rollen, die die Genehmigeraufgabe enthalten und gibt die Mitglieder dieser Rolle als Teilnehmer zurück.

Wenn Sie mehr als einen Teilnehmer-Resolver auswählen, berücksichtigt Identity Manager sie in dieser Rangordnung:

1. Benutzerdefiniert
2. Rolle
3. Filter
4. Gruppe

Identity Manager identifiziert den ersten Resolver, wendet ihn in dieser Rangordnung an und lässt die nachfolgenden Resolver unberücksichtigt.

Sie sollten nur einen Resolver gleichzeitig auswählen. Stellen Sie außerdem sicher, dass der Resolver korrekt konfiguriert ist, so dass Identity Manager die Teilnehmer richtig identifizieren kann.

Festlegen des Workflow-Ressourceskripts

Identity Manager verfügt über ein Skript mit dem Namen "IM Approvers", das Informationen zwischen Identity Manager und dem Workflow-Server weiterleitet.

Wenn eine Teilnehmerliste für eine Workflow-Aktivität erforderlich ist, leitet das Skript den Aktivitätsnamen, den Teilnehmeridentifizierer, der auf der Registerkarte "Benutzerinformationen" im WorkPoint-Dialogfenster "Aktivitätseigenschaften" angegeben ist, sowie alle sonstigen auf der Registerkarte "Benutzerdaten" angegebenen Informationen an Identity Manager weiter. Identity Manager sucht nach Teilnehmern und gibt die Liste zurück an das Skript. Das Skript leitet dann die Liste weiter an den Workflow-Server.

Wenn Sie eine neue Workflow-Prozessdefinition haben und die Workflow-Prozessaktivität eine Identity Manager-Workflow-Genehmigungsaufgabe ist, muss das IM-Genehmigerskript in der Registerkarte "Ressourcen" im WorkPoint-Dialogfenster "Aktivitätseigenschaften" angegeben sein.

So legen Sie das IM-Genehmigerskript im WorkPoint Designer fest

1. Klicken Sie in der Registerkarte "Ressourcen" auf "Auswählen".
2. Wählen Sie im Dialogfeld "Ressourcen" in der Dropdown-Liste die Option "Regel" aus. Diese Aktion listet die Regeln (Skripts) auf, die Sie mit der Aktivität verknüpfen können.

3. Wählen Sie den Skriptnamen "IM-Genehmiger" aus, und klicken Sie auf "Hinzufügen".
4. Klicken Sie auf "OK" und anschließend im Dialogfeld "Aktivitätseigenschaften" auf "Anwenden".

Hinweis: Verändern Sie nicht das IM-Genehmigerskript.

Festlegen von Teilnehmern für die Aufgabe "Benutzer zertifizieren"

Die Aufgabe "Benutzer zertifizieren" generiert das Ereignis "CertifyRoleEvent". Dieses Ereignis kann der Workflow-Genehmigung durch den vordefinierten Prozess "CertifyRoleApproveProcess" unterliegen.

Identity Manager umfasst außerdem den vordefinierten Teilnehmer-Resolver "CertifyRoleParticipantResolver", der standardmäßig in Ihrer Umgebung angezeigt wird. Teilnehmer an Aktivitäten im Prozess "CertifyRoleApprovalProcess" werden über "CertifyRoleParticipantResolver" festgelegt.

So erhalten Sie Informationen über die Teilnehmerkonfiguration:

1. Öffnen Sie die Management-Konsole, indem Sie die folgende URL in einen Browser eingeben:

   `http://hostname/iam/immanage`

   Hostname

   Definiert dem voll qualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist. Beispiel: myserver.mycompany.com:port.
2. Klicken Sie auf "Umgebungen" und wählen Sie anschließend den Namen der jeweiligen CA IdentityMinder-Umgebung aus.
3. Klicken Sie auf "Erweiterte Einstellungen" und anschließend auf "Sonstiges".
4. Definieren Sie Namen-Werte-Paare, die die Genehmiger für jede Rolle festlegen, die zertifiziert werden muss.
   - Verwenden Sie im Feld "Eigenschaften" das Format: *Rollen-Typ.Rollen-Name*

     Rollen-Typ muss einer dieser Rollen entsprechen: Admin, Zugriff, Bereitstellung.

     Rollen-Name ist der Name einer bestehenden Rolle.

     Der Rollen-Name und der Rollen-Typ müssen durch einen Punkt (.) voneinander getrennt werden.
   - Geben Sie im Feld "Wert" die IDs der Genehmiger an und trennen Sie die IDs mit einem Semikolon (;).

Im folgenden Beispiel kann die Benutzerzertifikation für folgende Rollen und durch folgende Teilnehmer genehmigt werden:

- jsmith01 und ajones19 können die Zertifikation für die Rolle "Benutzer-Manager" vornehmen.
- plewis12 ist der einzige Genehmiger für die Rolle "System-Manager".
- rtrevor8 und pkitt3 können die Zertifikation für die Rolle "Mein Zugriff" vornehmen.

Eigenschaft	Wert
admin. Benutzer-Manager	jsmith01;ajones19
admin.System-Manager	plewis12
access.Rolle "Mein Zugriff"	rtrevor8;pkitt3

Hinweis: Bei nicht festgelegten Rollen gibt es keine Genehmiger für das Ereignis "CertifyRoleEvent".

Prozesse im WorkPoint Designer

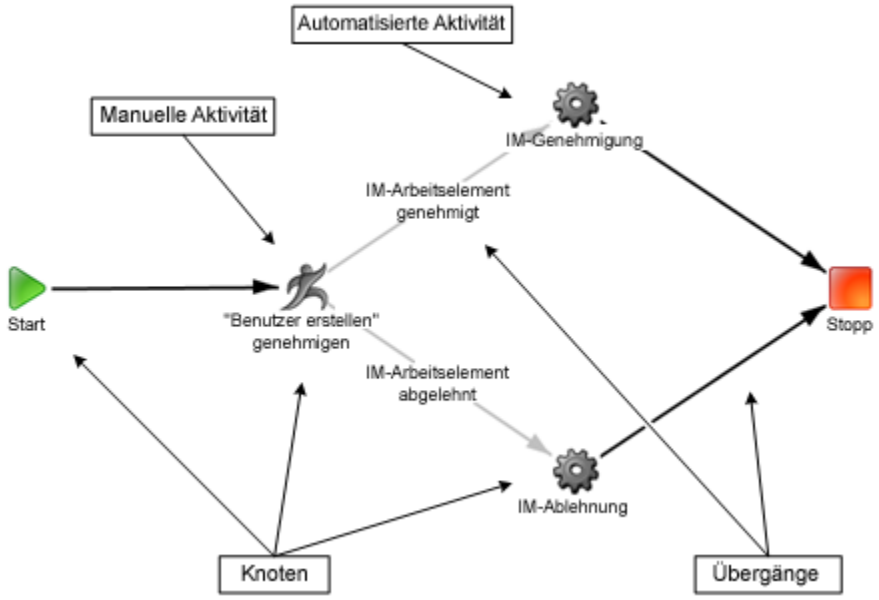
Im WorkPoint Designer können Sie die Standard-Workflow-Prozesse und Aktivitäten benutzerdefiniert anpassen, die in Identity Manager enthalten sind, und Sie können neue erstellen.

Dieses Dokument enthält Workflow-Informationen zu WorkPoint, die speziell für Identity Manager gelten. Vollständige Informationen hierzu finden Sie in der WorkPoint Designer-Dokumentation.

Hinweis: Wenn Sie einen Workflow-Prozess erstellen möchten, erstellen Sie am Besten eine Kopie eines bestehenden Identity Manager-Prozesses und passen den neuen Prozess an Ihre Bedürfnisse an. Ein auf diese Weise erstellter Workflow-Prozess umfasst standardmäßig Identity Manager-spezifische Elemente und Knoten sowie Transitionsskripts und automatisierte Aktivitäten.

WorkPoint-Prozessdiagramm

Das folgende Diagramm zeigt einen typischen Workflow-Prozess mit den mindestens erforderlichen Komponenten für einen Prozess, der eine Identity Manager-Aufgabe kontrolliert. Das Diagramm zeigt den vordefinierten Prozess "CreateUserApproveProcess", der die Ausführung der Aufgabe "Benutzer erstellen" kontrolliert.



WorkPoint-Prozesskomponenten

Der Workflow-Prozess enthält folgende Knoten und Transitionen:

Starten

Jeder Workflow-Prozess beginnt bei diesem Knoten.

Beenden

Jeder Workflow-Prozess endet bei diesem Knoten.

Manuelle Aktivität

Eine manuelle Aktivität erfordert die Genehmigung oder Ablehnung einer Identity Manager-Aufgabe durch einen Teilnehmer und muss denselben Namen haben, wie die Identity Manager-Workflow-Genehmigungsaufgabe.

Ein Workflow-Prozess, der eine Identity Manager-Aufgabe kontrolliert, muss mindestens eine manuelle Aktivität enthalten, die die Genehmigung für die Aufgabe anfordert.

Automatisierte Aktivität

Einer automatisierte Aktivität wird einem der beiden Skripts zugewiesen:

- Notify IM Approve: Informiert Identity Manager, die Identity Manager-Aufgabe unter Workflow-Kontrolle auszuführen.
- Notify IM Reject: Informiert Identity Manager, die Ausführung der Identity Manager-Aufgabe abzubrechen.

Generell wird das Skript "Notify IM Approve" aktiviert, wenn alle manuellen Aktivitäten genehmigt sind. Das Skript "Notify IM Reject" wird aktiviert, wenn eine manuelle Aktivität abgelehnt wird.

Bedingungslose Transition

Eine bedingungslose Transition ist ein Pfad von einem Knoten im Workflow-Prozess zum nächsten und ist mit keinem Bedingungsskript verknüpft.

Bedingte Transition

Eine bedingte Transition stellt einen alternativen Pfad von einem Knoten im Workflow-Prozess zum nächsten dar und ist mit einem Bedingungsskript verknüpft.

Ein Bedingungsskript bestimmt, ob die Transition durch die Bewertung des Ergebnisses einer verknüpften Aktivität erfolgt. Wenn das Skript den Wert "True" zurückgibt, wird die Transition ausgeführt, und der Prozess schreitet zum nächsten angezeigten Knoten weiter.

Es können auch zwei oder mehrere Bedingungsskripts den Wert "True" zurückgeben. Dadurch kann eine Aktivität parallel ausgeführt werden, da jedes Skript mit einer anderen Transition verknüpft ist.

Hinweis: Sie können bei bedingten Transitionen auch benutzerdefinierte Skripts verwenden. Weitere Anweisungen finden Sie im *Programmierhandbuch für Java*.

Eigenschaften manueller Aktivitäten

Identity Manager-spezifische Einstellungseigenschaften werden in folgender Tabelle aufgelistet. Diese Einstellungen werden in den genannten Registerkarten des Dialogfeldes "Aktivitätseigenschaften" im WorkPoint Designer definiert.

Registerkarte "Eigenschaft"	Beschreibung der Eigenschaften
Informationen	IM Approvers: In der Einschlussliste festgelegt. Dieses Skript leitet Informationen zwischen Identity Manager und dem Workflow-Server weiter.
Agenten	Nobody Auto Complete: Ist in der Asynchronliste festgelegt und mit dem Verfügbarkeitsstatus verknüpft. Dieses Skript bestimmt, ob eine Aktivität genehmigt werden soll, wenn kein Aktivitätsteilnehmer vorhanden ist.

Registerkarte "Eigenschaft"	Beschreibung der Eigenschaften
Benutzerdaten	Definieren die Namen-Werte-Paare, die Identity Manager zum Abrufen der Aktivitätsteilnehmer verwendet. Optional können Sie auch definieren, dass Daten an einen benutzerdefinierten Teilnehmer-Resolver weitergeleitet werden sollen.

Eigenschaften bedingter Transitionen

Die folgenden Standardskripte werden in der Registerkarte "Bedingung" des Dialogfeldes "Transitionseigenschaften" angezeigt:

IM WorkItem Approved

Gibt den Wert "True" zurück, wenn die verknüpfte Aktivität genehmigt wird. Der Workflow-Prozess geht weiter zum nächsten Knoten, der von der Transition angegeben wird.

IM WorkItem Rejected

Gibt den Wert "True" zurück, wenn die verknüpfte Aktivität abgelehnt wird. Der Workflow-Prozess geht weiter zum nächsten Knoten, der von der Transition angegeben wird.

Job- und Prozessinstanzen

Ein *Workflow-Prozess* definiert die Schritte, die getätigt werden müssen, bevor Identity Manager eine bestimmte Aufgabe abschließen kann. Ein *Job* ist eine Laufzeitinstanz eines Workflow-Prozesses.

Beispiel: Der Standard-Workflow-Prozess "CreateUserApproveProcess" definiert die notwendigen Schritte, damit ein neuer Benutzer genehmigt werden kann. Wenn ein neuer Benutzer in Identity Manager erstellt wird und die Aufgabe zur Genehmigung übermittelt wird, wird im WorkPoint Designer eine Jobinstanz "CreateUserApproveProcess" erstellt.

Sie können Jobs im WorkPoint Designer mit einer Benutzeroberfläche öffnen, anzeigen und ändern, die der zur Bearbeitung von Workflow-Prozessen sehr ähnlich ist.

Es können gleichzeitig mehrere Jobs existieren, die auf dem gleichen Prozess basieren.

Filtern von Jobs

WorkPoint Designer enthält eine Filterfunktion, mit der Sie nach Jobs auf Grundlage verschiedener Kriterien suchen können. Zum Beispiel können Sie nach Jobs suchen, die:

- auf einem oder mehreren ausgewählten Workflow-Prozessen basieren.
- über einen benutzerdefinierten Jobverweis oder eine eindeutige Job-ID verfügen.

- sich in einem bestimmten Zustand befinden (wie etwa aktiv, beendet oder angehalten).
- die innerhalb eines bestimmten Zeitraums erstellt oder gestartet wurden.

Hinweis: Weitere Anweisungen und Referenzinformationen zur Jobfilterung finden Sie in der WorkPoint Designer-Dokumentation.

Jobstatus und Eigenschaften

Wenn Sie einen Job öffnen wird das Workflow-Diagramm des Jobs angezeigt. Workflow-Aktivitätsknoten und Transitionen werden farbig dargestellt, um anzuzeigen, ob sie ausgeführt wurden.

Sie können sich Folgendes anzeigen lassen und gegebenenfalls ändern:

- Jobeigenschaften, einschließlich Informationen über Teilnehmer und Verlauf.
- Den Status eines offenen Jobs, zum Beispiel, ob er beendet ist.
- Eigenschaften von einzelnen Knoten und Transitionen in einem Job.

Eigenschaften von Aktivitäten und Arbeitselementen

Sie können sich Jobaktivitätseigenschaften und Prozessaktivitätseigenschaften anzeigen lassen und ggf. ändern, einschließlich:

- Informationen zum Aktivitätsstatus
- Informationen zur Aktivitätsgenehmigung
- Informationen zur Genehmigungsaufgabe (in WorkPoint Designer als *Arbeitselement* bezeichnet), z. B.:
  - Wenn kein Teilnehmer das Arbeitselement reserviert hat (wodurch das Element aus den Arbeitslisten der anderen Genehmiger entfernt wird), lautet der Status "Verfügbar" und es wird keine Benutzer-ID eines Teilnehmers angezeigt.
  - Wenn ein Teilnehmer das Arbeitselement reserviert, aber noch nicht abgeschlossen hat, lautet der Status "Offen" und die Benutzer-ID des Teilnehmers sowie der Reservierungszeitpunkt werden angezeigt.
  - Wenn das Arbeitselement abgeschlossen wurde, lautet der Status "Abgeschlossen". Die Benutzer-ID des Teilnehmers, der die Aufgabe unter Workflow-Kontrolle genehmigt oder abgelehnt hat, wird zusammen mit dem Abschlusszeitpunkt angezeigt.

Die spezifischen Arbeitselementeigenschaften umfassen:

- Der Name und der aktuelle Status des Arbeitselements
- Informationen zum Statusverlauf, einschließlich der Benutzer-IDs der für den jeweiligen Staus verantwortlichen Teilnehmer
- Informationen zu den autorisierten Arbeitselementteilnehmern

Hinweis: Weitere Informationen zu Job, Aktivität und Arbeitselementeigenschaften finden Sie in der Dokumentation zu WorkPoint Designer.

Workflow-Aktivitäten ausführen

In einem Workflow-Prozess wird eine manuelle Aktivität durch einen Benutzer durchgeführt, der als Aktivitätsteilnehmer bezeichnet wird, die ein der Genehmigungsaufgabe zugeordnetes Ereignis genehmigt oder ablehnt. Teilnehmer führen diese Aktivität in Identity Manager durch.

Folgende Vorgänge finden statt, wenn einer Aktivität, die einer Identity Manager-Genehmigungsaufgabe zugeordnet ist, durchgeführt wird:

1. Identity Manager benachrichtigt die Teilnehmer.
2. Ein Teilnehmer genehmigt die Aufgabe oder lehnt sie ab.
3. Der Workflow-Server schließt die Aktivität ab.

Suchen und Benachrichtigen der Teilnehmer

Wenn eine Workflow-Aktivität beginnt, die einer Identity Manager-Genehmigungsaufgabe zugeordnet ist, übergibt der Workflow-Server die Informationen zu den Aktivitätsteilnehmern an Identity Manager. Diese Informationen sind in den Aktivitätseigenschaften definiert. Identity Manager verwendet diese Informationen, um die Aktivitätsteilnehmer abzurufen und sie über eine anstehende Genehmigungsaufgabe zu benachrichtigen.

Nach der Indentifizierung der Teilnehmer fügt Identity Manager in den Arbeitslisten der einzelnen Teilnehmer ein neues Arbeitselement (die Genehmigungsaufgabe) hinzu. Optional sendet Identity Manager außerdem an alle Teilnehmer eine E-Mail-Benachrichtigung über das neue Arbeitselement.

Hinweis: Wenn die APPROVERS_REQUIRED-Aktivität auf "false" gesetzt ist und keine Teilnehmer gefunden werden, wird die Aufgabe standardmäßig als genehmigt betrachtet.

Hinweis: Ein Kreis in der Statusspalte zeigt an, dass die Genehmigungsaufgabe von allen Teilnehmern beansprucht werden kann. Ein Häkchen zeigt an, dass der Eigentümer der Arbeitsliste die Genehmigungsaufgabe akzeptiert, aber noch nicht angeschlossen hat.

Akzeptieren und Durchführen der Genehmigungsaufgabe

Nachdem die Teilnehmer gefunden sind, kann die Aktivität erst abgeschlossen werden, wenn ein Teilnehmer die Genehmigungsaufgabe akzeptiert und die in der Workflow-Kontrolle stehende Aufgabe entweder genehmigt oder ablehnt.

Ein Teilnehmer akzeptiert eine Genehmigungsaufgabe, indem er in der Workflow-Aktivitätskonsole auf den Namen des Arbeitselements klickt und dann "Element reservieren" auswählt. (Die Reservierung dieses Arbeitselements entfernt es aus den Arbeitslisten anderer Genehmiger.)

Indem ein Teilnehmer eine Genehmigungsaufgabe akzeptiert, verpflichtet er sich, die Entscheidung über die Genehmigung oder die Ablehung für die Aufgabe in der Workflow-Kontrolle zu treffen. Da eine Genehmigungsaufgabe nicht durch mehrere Teilnehmer akzeptiert werden kann, wird sie aus den Arbeitslisten der anderen Teilnehmer entfernt.

Nach dem Akzeptieren einer Genehmigungsaufgabe durch einen Teilnehmer wird ein Genehmigungsfenster angezeigt, in dem der Teilnehmer eine der folgenden Aktionen durchführen kann:

- Die Aufgabe unter Workflow-Kontrolle sofort genehmigen oder ablehnen.
- Die Genehmigungsaufgabe freigeben und für andere Teilnehmer verfügbar machen.
- Das Dialogfeld schließen und die Aktivität später abschließen. Um das oben angezeigte Dialogfeld "'Benutzer erstellen' genehmigen" erneut anzuzeigen, muss der Teilnehmer in seiner Arbeitsliste auf den Namen der Genehmigungsaufgabe klicken.

Darüber hinaus kann der Teilnehmer eventuell im Genehmigungsfenster vorhandene modifizierbare Felder aktualisieren. Sie können die in diesem Fenster angezeigten Felder beim Erstellen der Aufgabe editierbar machen.

Nachdem der Teilnehmer die Aufgabe unter Workflow-Kontrolle genehmigt oder abgelehnt hat, ist die Aktivität abgeschlossen und der Workflow-Prozess kann entlang des durch das Ergebnis der Aktivität vorgegebenen Pfads fortgesetzt werden. Dies wird im nächsten Abschnitt beschrieben.

Der Workflow-Server schließt die Aktivität ab.

Eine manuelle Aktivität wird im Designer-Fenster zusammen mit zwei oder mehr bedingten Transitionen angezeigt, die davon abgehen.

Jeder bedingten Transition ist ein Skript zugeordnet. Wenn ein Teilnehmer die Aktivität abschließt, wertet das Skript das Ergebnis der Aktivität aus. Das Ergebnis der Auswertung bestimmt, in welche Richtung der Prozess weiter läuft.

Die folgende Abbildung zeigt die Aktivität "'Benutzer erstellen' genehmigen" im Designer und die zugehörige Genehmigungsaufgabe mit demselben Namen in Identity Manager.

Wenn der Aktivitätsteilnehmer (oder Genehmiger) in Identity Manager auf die Schaltfläche "Genehmigen" bzw. "Ablehnen" klickt:

1. Die Aktivität "'Benutzer erstellen' genehmigen" wird in der Prozessjobinstanz beendet. Das den bedingten Transitionen zugeordnete Skript wertet das Ergebnis der Aktivität aus.
2. Die Jobinstanz wird fortgesetzt, abhängig davon, welche der bedingten Transitionen mit "true" ausgewertet wird:
   - Wenn die Aktivität genehmigt wurde, gibt das Skript "IM-Arbeitselement genehmigt" den Wert "true" zurück. Der Workflow bringt die Transition "IM-Arbeitselement genehmigt" zum nächsten Knoten. Die automatische Aktivität "IM-Genehmigung" benachrichtigt Identity Manager, dass die Aufgabe "Benutzer erstellen" ausgeführt werden soll.
   - Wenn die Aktivität genehmigt wurde, gibt das Skript "IM-Arbeitselement abgelehnt" den Wert "true" zurück. Der Workflow bringt die Transition "IM Arbeitselement genehmigt" zum nächsten Knoten. Die automatische Aktivität "IM-Ablehnung" benachrichtigt Identity Manager, dass die Aufgabe "Benutzer erstellen" ausgeführt werden soll.

Workpoint-Job-Ansicht

Sie können den Laufzeitstatus von Workpoint-Jobs in der Benutzerkonsole wie folgt anzeigen:

- Genehmigungsaufgaben
- Gesendete Aufgaben anzeigen

In neuen Umgebung enthalten alle Genehmigungsaufgaben standardmäßig die Registerkarte "Job anzeigen". Nur in dieser Version erstellte Ereignisse unterstützen das Anzeigen der Job-Ansichten in "Gesendete Aufgaben anzeigen" für alle Prozessdefinitionen, die für das ausgewählte Ereignis bzw. diese Aufgabe aufgerufen wurden. In früheren Versionen erstellte Ereignisse bieten keine Unterstützung für die Workpoint-Job-Anzeigefunktion.

Hinzufügen der Registerkarte "Job anzeigen" zu den vorhandenen Registerkarten für Genehmigungen

Für Genehmigungsaufgaben müssen Sie die neue Registerkarte "Job anzeigen" zu allen vorhandenen Aufgaben hinzufügen, um die Job-Ansicht für das Arbeitselement anzeigen zu können.

Hinweis: Neue Umgebungen enthalten diese Registerkarte für alle Genehmigungsaufgaben.

So fügen Sie die Registerkarte "Job-Ansicht" zu einer vorhandenen Aufgabe hinzu:

1. Führen Sie "ModifyAdminTask" von den Kategorien "Admin-Aufgaben" und "Rolle" aus, indem Sie "Admin-Aufgabe", "Admin-Aufgabe ändern" auswählen.
2. Klicken Sie auf "Suchen", wählen Sie eine Genehmigungsaufgabe aus (z. B. "Benutzer erstellen genehmigen") und klicken Sie auf "Auswählen".

   Die Seite "Benutzer erstellen genehmigen" des Dialogfeldes "Admin-Aufgabe ändern" wird angezeigt.
3. Klicken Sie auf die Registerkarte "Registerkarten", wählen Sie im Dropdown-Menü "Job anzeigen" (Job-Ansicht) aus, und klicken Sie auf "Senden".

   Die Registerkarte "Job anzeigen" wurde zur Genehmigungsaufgabe hinzugefügt.

   Wiederholen Sie diesen Vorgang für alle vorhandenen Genehmigungsaufgaben.

Konfigurieren der Registerkarte "Job anzeigen"

Konfigurieren Sie diese Registerkarte mit:

Name

Ein Name, den Sie der Registerkarte zuweisen.

Tag

Eine ID für die Registerkarte, die innerhalb dieser Aufgabe eindeutig ist. Sie muss mit einem Buchstaben oder Unterstrich beginnen und darf nur Buchstaben, Zahlen oder Unterstriche enthalten. Der Tag wird hauptsächlich zum Festlegen von Datenwerten durch XML-Dokumente oder HTTP-Parameter verwendet.

Registerkarte ausblenden

Verhindert, dass die Registerkarte in der Aufgabe sichtbar ist. Diese Option ist für Anwendungen praktisch, bei denen die Registerkarte zwar ausgeblendet werden soll, der Zugriff auf die Attribute auf der Registerkarte jedoch weiterhin möglich sein soll.

Job View

Diese Registerkarte zeigt die Job-Ansicht für das angegebene Arbeitselement.

Anzeigen der Registerkarte "Job anzeigen" für eine Genehmigungsaufgabe

Gehen Sie wie folgt vor, um die Registerkarte "Job anzeigen" für eine Genehmigungsaufgabe anzuzeigen.

So rufen Sie die Registerkarte "Job anzeigen" auf:

1. Wählen Sie im Dialogfeld "Arbeitsliste" die anzuzeigende Genehmigungsaufgabe aus
2. Klicken Sie auf die Registerkarte "Job anzeigen", um den Laufzeitstatus der Aufgabe anzuzeigen.

   Von hier aus können Sie die Aufgabe "Bestätigen", "Ablehnen", "Reservieren" oder die Registerkarte schließen.

Alternativ dazu können Sie auf die Registerkarte "Startseite" klicken und "Meine Arbeitsliste" anzeigen, um zum Dialogfeld "Arbeitsliste" zu wechseln.

Anzeigen eines Workflow-Jobs für Workflows auf Ereignisnebene

Gehen Sie zum Anzeigen eines Workflow-Jobs für Workflows auf Ereignisnebene in "Gesendete Aufgaben anzeigen" wie folgt vor.

So zeigen Sie einen Workflow-Job an:

1. Wählen Sie in der Registerkarte "Systeme" die Option "Gesendete Aufgaben anzeigen" aus, geben Sie Ihre Suchkriterien ein, und klicken Sie auf "Suchen".
2. Wählen Sie das Ereignis aus, und klicken Sie auf den Stift, um die Ereignisdetails anzuzeigen.
3. Wählen Sie unter "Ereignis-Workflow - Job-Ansicht" den Prozess aus, und klicken Sie auf den Stift, um die Job-Ansicht für dieses Ereignis anzuzeigen.

Anzeigen eines Workflow-Jobs für Workflows auf Aufgabenebene

Gehen Sie zum Anzeigen eines Workflow-Jobs für Workflows auf Aufgabenebene in "Gesendete Aufgaben anzeigen" wie folgt vor.

So zeigen Sie einen Workflow-Job an:

1. Wählen Sie in der Registerkarte "Systeme" die Option "Gesendete Aufgaben anzeigen" aus, geben Sie Ihre Suchkriterien ein, und klicken Sie auf "Suchen".
2. Wählen Sie die Aufgabe aus, und klicken Sie auf den Stift, um die Aufgabendetails anzuzeigen.

Wählen Sie unter "Aufgaben-Workflow - Job-Ansicht" den Prozess aus und klicken Sie auf den Stift, um die Job-Ansicht für diese Aufgaben anzuzeigen.

Richtlinienbasierter Workflow

Richtlinienbasierte Workflows ermöglichen Ihnen, basierend auf der Auswertung einer Regel ein Ereignis oder eine Admin-Aufgabe einer Workflow-Kontrolle zu unterstellen. Dies bedeutet, dass ein Ereignis oder eine Admin-Aufgabe nicht ständig einen Workflow-Prozess startet, sondern dass vielmehr der Workflow-Prozess nur dann ausgeführt wird und ein Arbeitselement generiert, wenn eine dem Ereignis bzw. der Admin-Aufgabe zugeordnete Regel erfüllt ist.

Eine *Genehmigungsregel* ist eine Bedingung, die bestimmt, ob ein Workflow-Prozess gestartet wird. Nach dem Start stellt der Workflow-Prozess das Ereignis oder die Admin-Aufgabe unter die Kontrolle des Workflows, indem er der Arbeitsliste eines Genehmigers ein Arbeitselement hinzufügt.

Eine *Genehmigungsrichtlinie* ist eine Kombination aus Genehmigungsregel, Regelauswertungstyp, Richtlinienreihenfolge, Richtlinienbeschreibung und Workflow-Prozess.

Beispielsweise können Sie, wenn Sie eine neue Gruppe erstellen, eine Genehmigungsrichtlinie definieren, die das Ereignis "CreateGroupEvent" der Workflow-Kontrolle unterstellt und nur dann ein Arbeitselement erstellt, wenn die neue Gruppe zu einer designierten übergeordneten Organisation gehört. Ist die neue Gruppe nicht Teil der Organisation, wird der Workflow-Prozess nicht ausgeführt, und es wird kein Arbeitselement erstellt.

Wenn ein Ereignis mehrere Regeln hat, muss der gesamte dem Ereignis zugeordnete Workflow-Prozess genehmigt werden, damit das Ereignis genehmigt wird. Entsprechend können Sie für eine Admin-Aufgabe eine Genehmigungsrichtlinie definieren, die die CreateGroupTask unter die Kontrolle des Workflows stellt und nur dann ein Arbeitselement erstellt, wenn der Name der neuen Gruppe mit "Vertrieb" beginnt. Wenn der Name der neuen Gruppe nicht mit "Vertrieb" beginnt, wird der Workflow-Prozess nicht ausgeführt, und es wird kein Arbeitselement erstellt.

Sie können eine Richtlinienregel erstellen, die immer oder nur dann ausgewertet wird, wenn sich ein angegebenes Attribut eines verwalteten Objekts, z. B. das Gehalt eines Mitarbeiters, ändert.

Hinweis: Wenn Genehmiger in früheren Versionen des richtlinienbasierten Workflows Änderungen an den Attributen durchgeführt haben, wurden diese Änderungen zur erneuten Genehmigung gesendet. Beim Genehmigen und Ablehnen auf Attributebene werden Änderungen immer nur einmal genehmigt. Das Arbeitselement wird niemals zur erneuten Genehmigung gesendet, auch wenn das in der Regel enthaltene Attribut geändert wird. Sobald ein Genehmiger eine Änderung genehmigt, wird das Arbeitselement nicht erneut angezeigt, bis eine neue Änderung gesendet oder die Aufgabe erneut gesendet wird.

Weitere Informationen:

Wokflow auf Ereignisebene (siehe Seite 290)
Workflow auf Aufgabenebene (siehe Seite 287)
Richtlinienreihenfolge (siehe Seite 345)
Regelauswertung (siehe Seite 343)

Standard-Workflow-Prozesse

Die Standard-Workflow-Vorlagen und die vordefinierten Workflow-Prozesse unterstützen Workflow-Regeln auf folgende Weise:

- **Prozessvorlagen** - Mit ihrer Hilfe lassen sich Genehmiger (oder Teilnehmer-Resolver) in der Benutzerkonsole konfigurieren.
- **Vordefinierte Workflow-Prozesse** - Sie erfordern die Konfiguration der Teilnehmer-Resolver in WorkPoint Designer.

Sie können auch benutzerdefinierte Workflow-Prozesse für die Verwendung mit Workflow-Regeln verwenden.

Weitere Informationen:

WorkPoint-Prozesse (siehe Seite 311)

Regelobjekte

Ein CA IdentityMinder-Administrator kann Genehmigungsrichtlinien für ein Ereignis oder eine Admin-Aufgabe basierend auf den folgenden Objekten erstellen. Die nachfolgend angegebenen Objekte sind die Objekte für ein Ereignis, wenn sie für ein bestimmtes Ereignis gelten und während der Ereignisausführung vorhanden sind:

- **Initiator der Aufgabe** - Der CA IdentityMinder-Administrator, der die Aufgabe ausführt.
- **Primäres Objekt des Ereignisses** - Das primäre Objekt, das dem Ereignis zugeordnet ist.
- **Sekundäres Objekt des Ereignisses** - Das sekundäre Objekt, das dem Ereignis relativ zum primären Objekt zugeordnet ist.

Die nachfolgend angegebenen Objekte sind die Objekte für eine Admin-Aufgabe:

- **Primäres Objekt der Aufgabe** - Das primäre Objekt, das der Aufgabe zugeordnet ist
- **Initiator der Aufgabe** - Der Identity Manager-Administrator, der die Aufgabe ausführt.
- **Verletzungen der Identitätsrichtlinie** - Die Regeln bei Verletzungen der Identitätsrichtlinie basieren auf dem Richtliniennamen der Identitätsrichtlinie, die die Verletzung verursacht hat, z. B. Richtlinienname EQUALS TitlePolicy. Die Verletzungsmeldung wird auf der Registerkarte "Aufgabendetails" des Genehmigungsfensters angezeigt, die der Registerkarte "Aufgabendetails" unter "Gesendete Aufgaben anzeigen" entspricht. Die SoD-Verletzungsmeldung wird unter der neuen Abschnittsüberschrift "Verletzung der Identitätsrichtlinie" angezeigt. Ein Genehmiger kann diese Meldungen anzeigen und die Aufgabe genehmigen oder ablehnen.

Regelauswertung

Richtlinienregeln können für ein Ereignis auf die folgenden zwei Weisen ausgewertet werden:

- Always (Immer)

  Eine Richtlinie mit dem Auswertungstyp "Always" (Immer) wird unabhängig davon aufgerufen, ob in der Richtlinie enthaltene Attribute geändert werden, wenn die Richtlinie als "True" (Wahr) ausgewertet wird. Im Genehmigungsfenster für ein Arbeitselement, das als Ergebnis des Richtlinienauswertungstyps "Always" (Immer) generiert wurde, kann ein Genehmiger alle bearbeitbaren Attribute ändern.

  Hinweis: Wenn der Genehmiger auf die Schaltfläche "Ablehnen" klickt, wird das Ereignis wie zuvor abgelehnt.

- Nur dann, wenn sich ein Attribut in der Genehmigungsbedingung ändert.

  Eine Richtlinie mit dem Auswertungstyp "OnChange" (Bei Änderung) wird nur dann aufgerufen, wenn die Richtlinie als "True" (Wahr) ausgewertet wird und eines der in der Richtlinie enthaltenen Attribute geändert wurde. Im Genehmigungsfenster für ein Arbeitselement, das als Ergebnis einer Richtlinie mit dem Auswertungstyp "OnChange" generiert wurde, kann der Genehmiger nur den Wert der in der Richtlinie enthaltenen Attribute ändern, sofern diese Attribute eine Lese-Schreib-Berechtigung für dieses Genehmigungsfenster besitzen. Alle anderen Attribute, die im Genehmigungsfenster vorhanden sind, besitzen nur Leseberechtigungen.

  Hinweis: Wenn der Genehmiger auf die Schaltfläche "Ablehnen" klickt, werden nur Änderungen abgelehnt, die an den in der Genehmigungsrichtlinie enthaltenen Attributen vorgenommen wurden, und die nächste Genehmigungsrichtlinie in der Reihenfolge wird ausgewertet.

  Diese Option gilt nur für das primäre Objekt des Ereignisses oder der Aufgabe.

Beachten Sie beispielsweise folgende Richtlinien, die alle für "ModifyUserEvent" in der Admin-Aufgabe "Benutzer ändern" gelten:

Richtlinie	Regel	Auswertung
Richtlinie1	Benutzer wobei (User ID = Smith01)	Always (Immer)
Richtlinie2	Benutzer wobei (Title = Manager)	Wenn das Attribut "Title" geändert wird
Richtlinie3	Benutzer wobei (Salary >= 80000)	Wenn das Attribut "Salary" geändert wird

Richtlinie1 wird jedes Mal unabhängig vom geänderten Attribut ausgewertet, wenn der Administrator die Aufgabe "Benutzer ändern" für den Benutzer "Smith01" aufruft.

Richtlinie2 wird ausgewertet, wenn der Administrator die Aufgabe "Benutzer ändern" aufruft, um das Attribut "Title" für ein beliebiges Benutzerobjekt zu ändern. Richtlinie2 ist "True" (Wahr), wenn der Titel in "Manager" geändert wird.

Richtlinie3 wird ausgewertet, wenn der Administrator die Aufgabe "Benutzer ändern" aufruft, um das Attribut "Salary" für ein beliebiges Benutzerobjekt zu ändern. Richtlinie3 ist "True" (Wahr), wenn das Gehalt in "80000" oder mehr geändert wird.

In diesem Beispiel sind Richtlinie1 und Richtlinie2 "True" (Wahr), wenn ein Administrator für den Benutzer "Smith01" die Aufgabe "Benutzer ändern" zum Ändern des Attributs "Title" in "Manager" verwendet, und die entsprechenden Workflow-Prozesse werden gestartet. In diesem Fall wird die Standardreihenfolge der Prioritäten verwendet.

Die bedingte Regelauswertung ermöglicht dem Genehmiger eines Arbeitselements das Ändern eines Attributs, das ein anderes Arbeitselement für dasselbe Ereignis beeinflusst, während das Ereignis noch aussteht. Dies ist nur für Genehmigungsrichtlinien möglich, deren Auswertungstyp "Always" (Immer) ist. Wenn ein Administrator im obigen Beispiel ein Attribut für den Benutzer "Smith01" ändert, ist Richtlinie1 "True" (Wahr), und ein Arbeitselement wird generiert. Der Genehmiger kann beim Bestätigen des von Richtlinie1 generierten Arbeitselements das Attribut "Salary" für "Smith01" in demselben Genehmigungsfenster ändern. In diesem Fall bestimmt der neue Wert für das Gehalt von "Smith01", ob Richtlinie3 ein Arbeitselement für dieselbe Instanz von "ModifyUserEvent" generiert. Wenn der Genehmiger das Gehalt in "90000" ändert, generiert Richtlinie3 ein neues Arbeitselement, das bestätigt werden muss, bevor das Ereignis selbst bestätigt wird. Die Standardreihenfolge der Prioritäten wird verwendet.

Weitere Informationen:

Richtlinienreihenfolge (siehe Seite 345)
Regelobjekte (siehe Seite 342)

Beispiel für eine Regelauswertung

Beachten Sie die folgenden Richtlinien, alle für ModifyUserEvent in der Admin-Aufgabe "Benutzer ändern":

Richtlinie	Regel	Auswertung
Richtlinie1	Benutzer wobei (User ID = Smith01)	Always (Immer)
Richtlinie2	Benutzer wobei (Title = Manager)	Wenn das Attribut "Title" geändert wird

Richtlinie	Regel	Auswertung
Richtlinie3	Benutzer wobei (Salary >= 80000)	Wenn das Attribut "Salary" geändert wird

Richtlinie1 wird jedes Mal unabhängig vom geänderten Attribut ausgewertet, wenn der Administrator die Aufgabe "Benutzer ändern" für den Benutzer "Smith01" aufruft.

Richtlinie2 wird ausgewertet, wenn der Administrator die Aufgabe "Benutzer ändern" aufruft, um das Attribut "Title" für ein beliebiges Benutzerobjekt zu ändern. Richtlinie2 ist "True" (Wahr), wenn der Titel in "Manager" geändert wird.

Richtlinie3 wird ausgewertet, wenn der Administrator die Aufgabe "Benutzer ändern" aufruft, um das Attribut "Salary" für ein beliebiges Benutzerobjekt zu ändern. Richtlinie3 ist "True" (Wahr), wenn das Gehalt in "80000" oder mehr geändert wird.

In diesem Beispiel sind Richtlinie1 und Richtlinie2 "True" (Wahr), wenn ein Administrator für den Benutzer "Smith01" die Aufgabe "Benutzer ändern" zum Ändern des Attributs "Title" in "Manager" verwendet, und die entsprechenden Workflow-Prozesse werden gestartet. In diesem Fall wird die Standardreihenfolge der Prioritäten verwendet.

Die bedingte Regelauswertung ermöglicht dem Genehmiger eines Arbeitselements das Ändern eines Attributs, das ein anderes Arbeitselement für dasselbe Ereignis beeinflusst, während das Ereignis noch aussteht. Dies ist nur für Genehmigungsrichtlinien möglich, deren Auswertungstyp "Always" (Immer) ist. Wenn ein Administrator im obigen Beispiel ein Attribut für den Benutzer "Smith01" ändert, ist Richtlinie1 "True" (Wahr), und ein Arbeitselement wird generiert. Der Genehmiger kann beim Bestätigen des von Richtlinie1 generierten Arbeitselements das Attribut "Salary" für "Smith01" in demselben Genehmigungsfenster ändern. In diesem Fall bestimmt der neue Wert für das Gehalt von "Smith01", ob Richtlinie3 ein Arbeitselement für dieselbe Instanz von "ModifyUserEvent" generiert. Wenn der Genehmiger das Gehalt in "90000" ändert, generiert Richtlinie3 ein neues Arbeitselement, das bestätigt werden muss, bevor das Ereignis selbst bestätigt wird. Die Standardreihenfolge der Prioritäten wird verwendet.

Richtlinienreihenfolge

Alle Genehmigungsrichtlinien enthalten das Feld "Richtlinienreihenfolge", mit dem die Priorität über einen positiven, ganzzahligen, aufsteigend sortierten Wert festgelegt wird. Von der Priorität der einzelnen Richtlinien hängt Folgendes ab:

- Die Reihenfolge, in der Genehmigungsregeln ausgewertet werden.
- Bei eingehaltenen Regeln die Reihenfolge, in der Workflow-Prozesse gestartet werden

Eine Richtlinie mit einer niedrigeren Ganzzahl hat eine höhere Priorität. Ihre Regel wird vor einer Richtlinie mit einer höheren Ganzzahl ausgewertet. Unter allen eingehaltenen Richtlinien für ein Ereignis oder eine Admin-Aufgabe startet die Richtlinie mit der höchsten Priorität als Erste ihren Workflow-Prozess.

Beispiel für die Richtlinienreihenfolge

Dieses einfache Beispiel zeigt, wie Richtlinienreihenfolgen funktionieren. In diesem Beispiel wird vorausgesetzt, dass die Richtlinien immer ausgewertet werden.

Falls ein Ereignis über mehrere Richtlinien verfügt, die immer ausgewertet werden, gilt das Ereignis nur dann als bestätigt, wenn alle Richtlinien bestätigt werden. Wenn jedoch eine dem Ereignis zugeordnete Richtlinie abgelehnt wird, deren Richtlinien-Auswertungstyp ALWAYS (Immer) ist, wird auch das Ereignis selbst abgelehnt.

Hinweis: Wenn der Auswertungstyp einer dem Ereignis zugeordneten Richtlinie "Onchange" ist, werden nur die Änderungen an den in dieser Richtlinie enthaltenen Attributen abgelehnt. Das Ereignis selbst wird nicht abgelehnt und die darauf folgende Richtlinie wird ausgewertet.

In diesem Beispiel ist der Richtlinien-Auswertungstyp von Richtlinie1, Richtlinie2 und Richtlinie3 jeweils ALWAYS. Richtlinie1 wird als "Falsch" ausgewertet, der Workflow-Prozess "Prozess1" wird nicht ausgeführt, und für Benutzer1 wird kein Arbeitselement generiert. Die Ereigniskontrolle wird umgehend an Richtlinie2 übergeben. Richtlinie2 und Richtlinie3 werden beide als "Wahr" ausgewertet. Auf Grund seiner höheren Priorität wird der Workflow-Prozess "Prozess2" als Erstes ausgeführt und generiert ein Arbeitselement für Benutzer2.

Falls Benutzer2 das Arbeitselement bestätigt, wird Workflow-Prozess "Prozess3" ausgeführt und ein Arbeitselement für Benutzer3 generiert, der dieses Arbeitselement bestätigen muss, damit das Ereignis selbst bestätigt wird. Diese Aktionen werden in der folgenden Tabelle aufgeführt:

Priorität	Richtlinie	Ergebnis	Workflow	Genehmiger	Aktion
1	Richtlinie1	Falsch	Prozess1	Benutzer1	—
2	Richtlinie2	Wahr	Prozess2	Benutzer2	Bestätigt
3	Richtlinie3	Wahr	Prozess3	Benutzer3	Bestätigt

Wie in der folgenden Tabelle dargestellt, wird, falls Benutzer2 das Arbeitselement ablehnt, das Ereignis selbst abgelehnt. Für Benutzer3 wird kein Arbeitselement generiert.

Priorität	Richtlinie	Ergebnis	Workflow	Genehmiger	Aktion
1	Richtlinie1	Falsch	Prozess1	Benutzer1	—
2	Richtlinie2	Wahr	Prozess2	Benutzer2	Abgelehnt
3	Richtlinie3	Wahr	Prozess3	Benutzer3	—

Der Auswertungstyp von Richtlinie1, Richtlinie2 und Richtlinie3 ist jeweils ONCHANGE. Wenn Benutzer2 das Arbeitselement ablehnt, werden nur die Änderungen der in Richtlinie2 enthaltenen Attribute abgelehnt. Anschließend wird Richtlinie3 ausgewertet und Workflow-Prozess3 ausgeführt, der ein Arbeitselement für Benutzer3 generiert. Wenn Benutzer3 das Arbeitselement ablehnt, wird das Ereignis genauso abgelehnt wie alle Änderungen an diesem Ereignis. Wenn Benutzer3 das Arbeitselement genehmigt, wird auch das Ereignis genehmigt und die in Richtlinie3 enthaltenen Attributänderungen werden beibehalten.

Priorität	Richtlinie	Ergebnis	Workflow	Genehmiger	Aktion
1	Richtlinie1	Falsch	Prozess1	Benutzer1	—
2	Richtlinie2	Wahr	Prozess2	Benutzer2	Abgelehnt
3	Richtlinie3	Wahr	Prozess3	Benutzer3	Bestätigt

Richtlinienbeschreibung

Ein optionales, nicht durchsuchbares Zeichenfolgenbeschreibungsattribut wurde zum verwalteten Objekt der Genehmigungsrichtlinie hinzugefügt und wird in resultierenden Arbeitselementen angezeigt.

Größtmögliche Anzahl von unterstützten Zeichen: 255 Zeichen

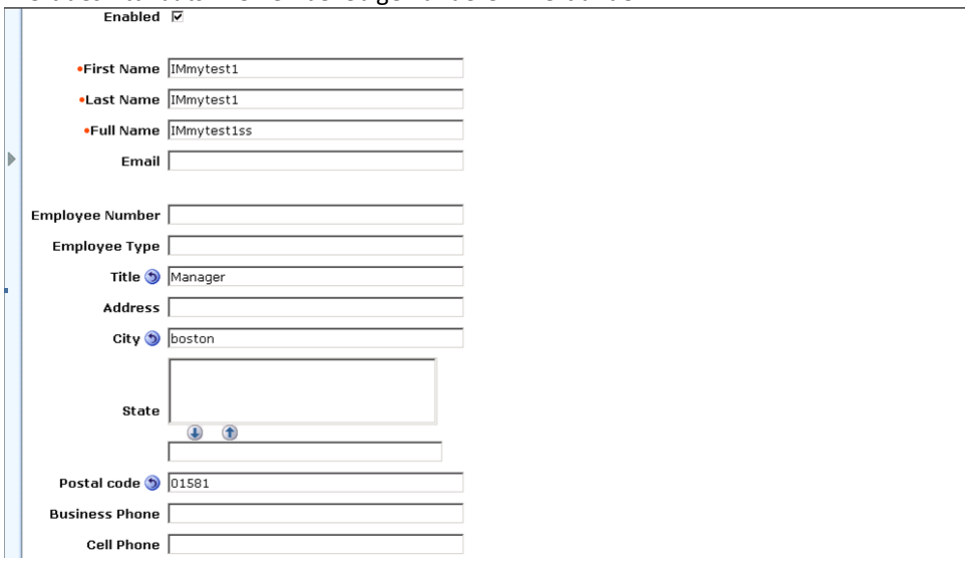
Sie können für die Beschreibung Bündel-/Schlüsselinformationen im folgenden Format eingeben:

```
$ (bundle=<voll qualifizierter Ressourcenbündelname> : key=<Schlüssel>)
```

Hervorheben geänderter Attribute in Genehmigungsfenstern

Damit ein Genehmiger weiß, welche Attribute geändert wurden, oder um bei Bedarf die an diesen Attributen vorgenommenen Änderungen rückgängig zu machen, wurde im Genehmigerprofilfenster ein Symbol zum Rückgängigmachen hinzugefügt, das dem Genehmiger anzeigt, dass das betreffende Attribut geändert wurde.

Der Genehmiger kann den ursprünglichen Wert der bearbeitbaren Attribute anzeigen, indem er auf die Schaltfläche zum Rückgängigmachen klickt, und darüber hinaus den Wert des Attributs in einen beliebigen anderen Wert ändern.



Genehmigungsrichtlinien und mehrwertige Attribute

Wenn eine Regel für ein mehrwertiges Attribut eingerichtet wurde, gab es keine Möglichkeit, festzulegen, dass diese Regel nur für neu hinzugefügte oder entfernte Werte für das mehrwertige Attribut gelten soll. Dies wird jetzt durch das Überprüfen des Richtlinienauswertungstyps für eine auf einem mehrwertigen Attribut basierende Regel erreicht. Wenn der Regelauswertungstyp "Onchange" (Bei Änderung) ist, kann diese Regel nur auf die neu hinzugefügten oder entfernten Werte des mehrwertigen Attributs angewendet werden und nicht auf alle Werte des mehrwertigen Attributs. Wenn die Regel auf allen Werten des mehrwertigen Attributs basieren muss, unabhängig davon, ob sie neu hinzugefügt oder entfernt wurden, muss der Auswertungstyp für diese Regel "Always" (Immer) sein.

Änderungen, die an mehrwertigen Attributen vorgenommen werden, werden im Profilfenster durch ein Symbol zum Rückgängigmachen hervorgehoben. Wenn eine Regel als "true" (wahr) ausgewertet wurde, da ein neuer Wert zu einem mehrwertigen Attribut hinzugefügt bzw. entfernt wurde, werden dem Genehmiger, der diese Änderung genehmigt, ALLE im mehrwertigen Attribut enthaltenen Werte angezeigt. Durch Klicken auf das Symbol "Rückgängig" wird der Wert für das entsprechende Attribut auf den ursprünglichen Wert zurückgesetzt. Wenn ein Genehmiger die entfernten Werte sehen möchte, kann er auf das Symbol "Rückgängig" klicken, um die ursprünglichen Werte anzuzeigen. Durch Klicken auf das Symbol zum Wiederholen werden die neuen Werte angezeigt, so dass der Genehmiger unterscheiden kann, bei welchen Werten es sich um die entfernten Werte und bei welchen um die hinzugefügten Werte handelt. Durch Klicken auf die Schaltfläche "Genehmigen" werden alle an diesem mehrwertigen Attribut vorgenommenen Änderungen genehmigt. Durch Klicken auf die Schaltfläche "Ablehnen" werden alle an diesem mehrwertigen Attribut vorgenommenen Änderungen abgelehnt. Alle nachfolgenden Regeln, die zu diesem mehrwertigen Attribut gehören, werden nur dann ausgewertet, wenn eine neue Wertedifferenz für dieses mehrwertige Attribut besteht.

Hinweis: Bei Regeln, die auf mehrwertigen Attributen basieren, sind die im mehrwertigen Attribut enthaltenen Werte die tatsächlichen Werte und nicht die Anzeigewerte. Beispielsweise ist "Massachusetts" der Anzeigewert für den US-Bundesstaat MA. Beim Erstellen einer Genehmigungsrichtlinie, die auf dem Bundesstaat-Attribut (state) basiert, sollte die Regel wie folgt lauten: state=MA.

Beachten Sie die folgenden Beispielrichtlinien, alle für ModifyUserEvent in der Admin-Aufgabe "Benutzer ändern":

Richtlinie	Regel	Auswertung
Richtlinie1	Benutzer wobei (State = MA)	OnChange
Richtlinie2	Benutzer wobei (state = DC)	Always (Immer)

Richtlinie1 wird jedes Mal ausgewertet, wenn ein Administrator die Aufgabe "Benutzer ändern" aufruft, um das Bundesstaat-Attribut zu ändern. Die Richtlinie wird als "True" (Wahr) ausgewertet, wenn der Wert "MA" zum Bundesstaat-Attribut hinzugefügt oder daraus entfernt wird.

Richtlinie2 wird jedes Mal ausgewertet, wenn der Administrator die Aufgabe "Benutzer ändern" für einen Benutzer aufruft, dessen Bundesstaat den Wert "DC" enthält.

Attribute werden auf Workflow-Genehmigungsfenstern als geändert hervorgehoben

Auf einem Genehmigungsfenster können zusätzliche Attribute als verändert hervorgehoben sein, selbst wenn ein Administrator sie in der ursprünglichen Aufgabe nicht verändert hat. Dies ist darauf zurückzuführen, dass das Fenster Skripte enthalten kann, die für die Änderung eines anderen Attributs die Werte mehrerer Attribute verändern können, die als Teil der Bildschirminitialisierung oder Bildschirmvalidierung auf dem Fenster enthalten sind.

Richtlinienbeispiele

Die folgenden Fallbeispiele demonstrieren, wie Sie Workflow-Genehmigungsrichtlinien für ein Ereignis anwenden können:

Beispiel 1:

Anwendungsfall - Ein Administrator ändert das Konto einer relationalen Datenbank, das einem Mitarbeiter gehört.

Admin-Aufgabe - ModifyMSSQLAccount

Ereignis - ModifyMSSQLAccountEvent

Genehmigungsregel - Benutzer wobei (Title = RDBAcctManager)

Workflow-Prozess - ModAcctApproval (benutzerdefinierter Workflow-Prozess)

Objekt - Initiator der Aufgabe

Auswertung - Regel immer auswerten

Beispiel 2:

Anwendungsfall - Ein Administrator ändert aufgrund einer Gehaltserhöhung das Gehalt eines Mitarbeiters.

Admin-Aufgabe – Benutzer ändern

Ereignis - ModifyUserEvent

Genehmigungsregel - Benutzer wobei (Salary >= 100000)

Workflow-Prozess - SalaryChangeApproval (benutzerdefinierter Workflow-Prozess)

Objekt – Primäres Objekt des Ereignisses (Benutzer)

Auswertung - Auswertung nur bei Änderungen des Attributs "Gehalt"

Beispiel 3:

Anwendungsfall - Ein Administrator fügt der Gruppe "Contractors" einen Benutzer hinzu, wenn sich der Titel des Benutzers in "Contractor" ändert. Dieses Beispiel könnte in zwei Genehmigungsrichtlinien unterteilt werden:

Richtlinie 1:

Admin-Aufgabe – Benutzer ändern

Ereignis - ModifyUserEvent

Genehmigungsregel - Benutzer wobei (Title = Contractor)

Workflow-Prozess – SingleStepApproval (Standard-Prozessvorlage)

Objekt – Primäres Objekt des Ereignisses (Benutzer)

Auswertung - Auswertung nur bei Änderungen des Attributs "Titel"

Richtlinie 2:

Admin-Aufgabe - Gruppe ändern (oder Gruppenmitgliedschaft ändern)

Ereignis - AddToGroup

Genehmigungsregel - Gruppe wobei (Group Name = Contractors)

Workflow-Prozess – SingleStepApproval (Standard-Prozessvorlage)

Objekt - Sekundäres Objekt des Ereignisses (der Gruppe)

Auswertung - Regel immer auswerten

Die folgenden Fallbeispiele demonstrieren, wie Sie Workflow-Genehmigungsrichtlinien für eine Aufgabe anwenden können:

Beispiel 1:

Anwendungsfall - Ein Administrator ändert ein Active Directory-Konto, das einem Mitarbeiter gehört.

Admin-Aufgabe - ModifyActiveDirectoryAccount

Objekt - Initiator der Aufgabe

Genehmigungsregel - Benutzer wobei (Title = ActiveDirectoryManager)

Workflow-Prozess - Einzelschritt-Genehmigung

Auswertung - Regel immer auswerten

Beispiel 2:

Anwendungsfall - Ein Administrator ändert einen Benutzer, dessen Mitarbeitercode "HighSecurity" ist.

Admin-Aufgabe – Benutzer ändern

Objekt - Primäres Objekt der Aufgabe

Genehmigungsregel - Benutzer wobei (employeenumber = HighSecurity)

Workflow-Prozess - Einzelschritt-Genehmigung

Auswertung - Regel immer auswerten

Beispiel 3:

Anwendungsfall - Ein Administrator ändert einen Benutzer zur Zuordnung der Admin-Rollen CheckApprover und CheckSigner.

Admin-Aufgabe – Benutzer ändern

Objekt - Verletzung der Identitätsrichtlinie

Genehmigungsregel - Identitätsrichtlinie wobei (Name = CheckRoles)

Workflow-Prozess - Einzelschritt-Genehmigung

Auswertung - Regel immer auswerten

Konfigurieren des richtlinienbasierten Workflows für Ereignisse

Die Vorgehensweise beim Konfigurieren eines richtlinienbasierten Workflows entspricht der für das Konfigurieren eines Workflows auf Ereignisebene. Hinzu kommen Schritte für das Definieren der Genehmigungsrichtlinien, die bestimmen, ob der Workflow ausgeführt wird.

So konfigurieren Sie einen richtlinienbasierten Workflow

1. Wählen Sie in der Benutzerkonsole die Optionen "Rollen und Aufgaben", "Admin-Aufgaben" und "Admin-Aufgabe ändern" (oder "Admin-Aufgabe erstellen") aus.

   Es wird ein Fenster zur Auswahl der Admin-Aufgabe angezeigt.

2. Suchen Sie die Aufgabe, die Sie der Workflow-Kontrolle unterstellen möchten, und klicken Sie auf "Auswählen".

   Das Fenster "Admin-Aufgabe ändern (oder erstellen)" wird angezeigt.

3. Überprüfen Sie auf der Registerkarte "Profil", ob "Workflow aktivieren" aktiviert ist.

4. Wählen Sie in der Registerkarte "Ereignisse" ein Ereignis aus, das einer Prozessvorlage zugeordnet werden soll.

   Das Fenster für die Workflow-Zuordnung wird angezeigt.

5. Wählen Sie das Optionsfeld "Richtlinien-basierend" aus, und klicken Sie anschließend auf "Hinzufügen".

   Das Fenster "Genehmigungsrichtlinie" wird angezeigt.

6. Konfigurieren Sie eine Genehmigungsrichtlinie (siehe Seite 356).

7. Konfigurieren Sie die für den ausgewählten Workflow-Prozess erforderlichen Teilnehmer-Resolver.

   Die Teilnehmeranforderungen werden dem Prozess hinzugefügt.

8. Klicken Sie auf "OK".

   CA IdentityMinder speichert Ihre Workflow-Konfiguration auf Ereignisebene.

9. Klicken Sie auf "Senden".

   CA IdentityMinder verarbeitet die Aufgabenänderung.

Hinweis: Die Workflow-Prozessliste enthält Prozesse für die Verwendung sowohl mit der Vorlagen- als auch mit der WorkPoint-Methode:

- Bei Auswahl einer Vorlagenmethode (entweder SingleStepApproval oder TwoStageApprovalProcess) wird die Seite erweitert, damit die Teilnehmer-Resolver konfiguriert werden können.
- Bei Auswahl eines Prozesses mit der WorkPoint-Methode wird die Seite nicht erweitert. Teilnehmer-Resolver werden in WorkPoint Designer konfiguriert.

Weitere Informationen:

Teilnehmer-Resolver: WorkPoint-Methode (siehe Seite 319)
Konfigurieren einer Genehmigungsrichtlinie (siehe Seite 356)

Konfigurieren des richtlinienbasierten Workflows für Aufgaben

Die Vorgehensweise beim Konfigurieren eines richtlinienbasierten Workflows für Aufgaben entspricht der für das Konfigurieren eines Workflows auf Aufgabenebene. Hinzu kommen Schritte für das Definieren der Genehmigungsrichtlinien, die bestimmen, ob der Workflow ausgeführt wird.

So konfigurieren Sie einen richtlinienbasierten Workflow

1. Wählen Sie in der Benutzerkonsole die Optionen "Rollen und Aufgaben", "Admin-Aufgaben" und "Admin-Aufgabe ändern" (oder "Admin-Aufgabe erstellen") aus.

   Es wird ein Fenster zur Auswahl der Admin-Aufgabe angezeigt.

2. Suchen Sie die Aufgabe, die Sie der Workflow-Kontrolle unterstellen möchten, und klicken Sie auf "Auswählen".

   Das Fenster "Admin-Aufgabe ändern (oder erstellen)" wird angezeigt.

3. Überprüfen Sie auf der Registerkarte "Profil", ob "Workflow aktivieren" aktiviert ist

4. Klicken Sie auf der Registerkarte "Profil" auf das Stift-Symbol neben dem Feld "Workflow-Prozess"

   Das Fenster für die Workflow-Zuordnung wird angezeigt.

5. Wählen Sie das Optionsfeld "Richtlinien-basierend" aus, und klicken Sie anschließend auf "Hinzufügen".

   Das Fenster "Genehmigungsrichtlinie" wird angezeigt.

6. Konfigurieren Sie eine Genehmigungsrichtlinie (siehe Seite 356).

7. Konfigurieren Sie die für den ausgewählten Workflow-Prozess erforderlichen Teilnehmer-Resolver.

   Die Teilnehmeranforderungen werden dem Prozess hinzugefügt.

8. Klicken Sie auf "OK".

   CA Identity Manager speichert Ihre Workflow-Konfiguration auf Aufgabenebene.

9. Klicken Sie auf "Senden".

   CA Identity Manager verarbeitet die Aufgabenänderung.

Hinweis: Die Workflow-Prozessliste enthält Prozesse zur Verwendung mit der Vorlagenmethode für den richtlinienbasierten Workflow auf Aufgabenebene:

- Bei Auswahl einer Vorlagenmethode (entweder SingleStepApproval oder TwoStageApprovalProcess) wird die Seite erweitert, damit die Teilnehmer-Resolver konfiguriert werden können.

Weitere Informationen:

Konfigurieren einer Genehmigungsrichtlinie (siehe Seite 356)

Konfigurieren einer Genehmigungsrichtlinie

Das Konfigurieren einer Genehmigungsrichtlinie für ein Ereignis oder eine Aufgabe umfasst die folgenden Schritte.

1. Wählen Sie ein zu testendes Objekt aus.
2. Definieren Sie eine Genehmigungsregel für das Objekt.
3. Entscheiden Sie für primäre Objekte, ob dies eine bedingte Auswertung ist.
4. Geben Sie die Reihenfolge der Richtlinienauswertung ein.
5. Konfigurieren Sie einen Workflow-Prozess, der ausgeführt werden soll, wenn die Regel zutrifft.

So konfigurieren Sie eine Genehmigungsrichtlinie:

1. Wählen Sie aus der Dropdown-Liste des Bildschirms "Genehmigungsrichtlinie" ein Objekt für die zu überprüfende Regel aus.

   Das Fenster ändert sich gemäß Ihrer Auswahl.
2. Wählen Sie aus der neuen Dropdown-Liste neben dem Objektnamen eine Vorlage für Bedingungsausdrücke aus.

   Das Fenster ändert sich gemäß Ihrer Auswahl.
3. Erstellen und bearbeiten Sie Ihren Bedingungsausdruck nach Bedarf.
4. Wählen Sie das Optionsfeld "Regelauswertung" aus, um anzugeben, ob die Regel immer ausgewertet werden soll, oder nur dann, wenn sich ein Attribut in der Genehmigungsbedingung ändert.
5. Geben Sie eine positive Ganzzahl ein, um die Reihenfolge der Richtlinienauswertung festzulegen, wenn es mehrere Richtlinien für das Ereignis gibt.
6. Wählen Sie den Workflow-Prozess aus, der ausgeführt wird, wenn die Regel zutrifft, und konfigurieren Sie ihn.
7. Klicken Sie auf "OK", um die Genehmigungsrichtlinie zu speichern.

Weitere Informationen:

Konfigurieren des Workflow auf Ereignisebene - Vorgehensweise (siehe Seite 292)
Konfigurieren des richtlinienbasierten Workflows für Ereignisse (siehe Seite 353)
Konfigurieren des richtlinienbasierten Workflows für Aufgaben (siehe Seite 355)

Status des richtlinienbasierten Workflows

Mit Hilfe folgender Standardsystemtools können CA IdentityMinder-Administratoren den Status von Aufgaben anzeigen, die Workflow-Genehmigungsrichtlinien enthalten:

- Registerkarte "Gesendete Aufgaben anzeigen"
- Registerkarte "Benutzerverlauf"
- Berichte und Protokolle

Zu den Informationen zu gesendeten Aufgaben und zum Aufgabenverlauf gehören:

- Aufgaben- und Ereignisinformationen
- Informationen zum Workflow und zu Genehmigungsregeln
- Ergebnisse der Auswertung von Genehmigungsregeln

Weitere Informationen zum Verlauf gesendeter Aufgaben finden Sie in der Dokumentation zur Registerkarte "System".

Weitere Informationen:

Beschreibung des Ereignisstatus (siehe Seite 589)
Aufgabenstatus in CA IdentityMinder (siehe Seite 582)

Globale, richtlinienbasierte Workflow-Zuordnung auf Ereignisebene

Ein Ereignis kann über die Managementkonsole einem Workflow-Prozess zugeordnet oder mit richtlinienbasierten Workflow-Genehmigungsrichtlinien in einer bestimmten Aufgabe verknüpft werden. Administratoren können mit Hilfe der neuen Aufgabe "Auf globaler Richtlinie basierter Workflow für Ereignisse konfigurieren" eine richtlinienbasierte Workflow-Zuordnung für Ereignisse auf der Umgebungsebene einrichten. Anders als beim Einrichten eines richtlinienbasierten Workflows für ein Ereignis in einer Admin-Aufgabe werden die konfigurierten richtlinienbasierten Workflow-Zuordnungen auf alle Aufgaben angewendet, die das Ereignis generieren.

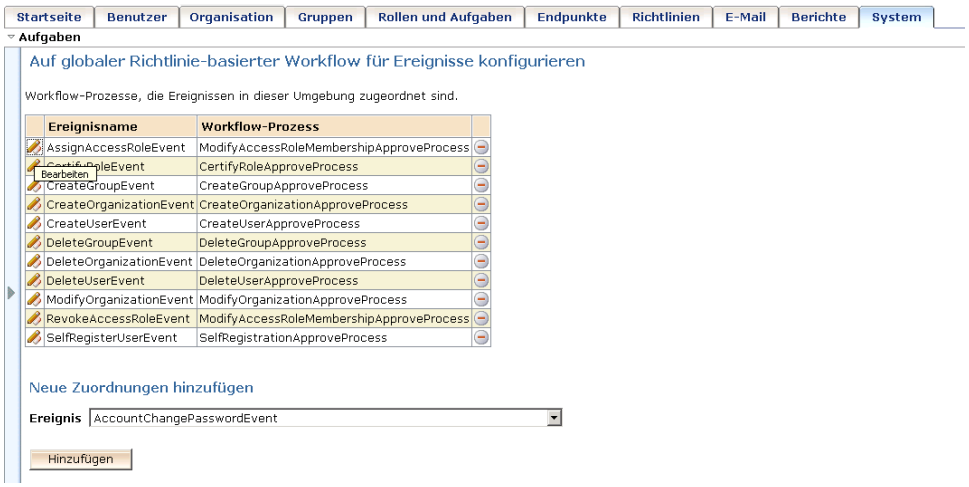
Hinweis: Die Aufgabe "Auf globaler Richtlinie basierter Workflow für Ereignisse konfigurieren" funktioniert nur, wenn der Workflow aktiviert ist. Wenn diese Aufgabe bei deaktiviertem Workflow ausgeführt wird, wird ein Fehler ausgegeben.

Diese Aufgabe wurde zur Registerkarte "System" hinzugefügt. Wenn eine Aufgabe gesendet wird, wird der Workflow-Prozess jedes Ereignisses in dieser Aufgabe auf die folgende Weise abgerufen:

Jeder für das Ereignis für diese Admin-Aufgabe konfigurierte Workflow hat Vorrang. Ein Ereignis kann für einen richtlinienbasierten oder einen nicht richtlinienbasierten Workflow konfiguriert werden. Wenn ein richtlinienbasierter Workflow für das Ereignis für diese Admin-Aufgabe konfiguriert ist, wird der der Richtlinie zugeordnete Workflow-Prozess aufgerufen. Wenn keine Regel übereinstimmte, wird kein Workflow für das Ereignis aufgerufen. Wenn ein nicht richtlinienbasierter Workflow für das Ereignis für diese Admin-Aufgabe konfiguriert ist, wird ebenfalls der der Richtlinie zugeordnete Workflow-Prozess aufgerufen. Wenn für das Ereignis für diese Admin-Aufgabe kein Workflow konfiguriert wurde, hat die globale Workflow-Konfiguration für dieses Ereignis Vorrang.

Aufgabenfenster "Auf globaler Richtlinie basierter Workflow für Ereignisse konfigurieren"

Die Aufgabe "Auf globaler Richtlinie basierter Workflow für Ereignisse konfigurieren" ermöglicht einem Administrator die Konfiguration eines richtlinienbasierten oder nicht richtlinienbasierten Workflows für alle Ereignisse in der aktuellen Umgebung. Wenn die Aufgabe angeklickt wird, wird die standardmäßige Ereigniszuordnung zu Workflow-Prozessdefinitionen angezeigt. Jede Ereigniszuordnung kann geändert oder gelöscht werden, und es können neue Ereigniszuordnungen für Ereignisse hinzugefügt werden, die noch nicht konfiguriert wurden.



Dieses Fenster enthält die folgenden Felder:

Workflow-Prozesse, die Ereignissen in dieser Umgebung zugeordnet sind.

Gibt die mit Genehmigungsrichtlinien verknüpften Workflow-Prozesse an.

Neue Zuordnungen hinzufügen

Gibt eine Genehmigungsrichtlinie an, die einem Workflow-Prozess zugeordnet werden soll.

Schaltfläche "Hinzufügen"

Fügt die neue Zuordnung hinzu.

Wenn Sie eine Zuordnung hinzufügen oder ändern, wird das Fenster für die Workflow-Zuordnung angezeigt, in dem Sie die Prozesszuordnungen und Genehmigungsrichtlinien auswählen können. Das Verhalten ist dasselbe wie bei der Workflow-Konfiguration auf Ereignisebene. Wenn Sie auf der Seite für die Workflow-Zuordnungen auf die Schaltfläche "Hinzufügen" klicken, wird eine andere Seite angezeigt, auf der Sie eine Genehmigungsrichtlinie konfigurieren können.

Weitere Informationen:

Konfigurieren des richtlinienbasierten Workflows für Ereignisse (siehe Seite 353)
Konfigurieren einer Genehmigungsrichtlinie (siehe Seite 356)

Auf globaler Richtlinie basierter Workflow für Ereignisse konfigurieren

Konfigurieren Sie diese Registerkarte für einen globalen, richtlinienbasierten Workflow für Ereignisse.

Name

Ein Name, den Sie der Registerkarte zuweisen.

Tag

Eine ID für die Registerkarte, die innerhalb dieser Aufgabe eindeutig ist. Sie muss mit einem Buchstaben oder Unterstrich beginnen und darf nur Buchstaben, Zahlen oder Unterstriche enthalten. Das Tag wird hauptsächlich zum Festlegen von Datenwerten durch XML-Dokumente oder HTTP-Parameter verwendet.

Registerkarte ausblenden

Verhindert, dass die Registerkarte in der Aufgabe sichtbar ist. Diese Option ist für Anwendungen praktisch, bei denen die Registerkarte zwar ausgeblendet werden soll, der Zugriff auf die Attribute auf der Registerkarte jedoch weiterhin möglich sein soll.

Benutzersuchfenster

Definiert das Suchfenster, das zum Anzeigen von Benutzern verwendet wird.

Benutzerlistenfenster

Definiert das Fenster, welches die Spalten und die Sortierung auf dieser Registerkarte bestimmt.

Gruppensuchfenster

Definiert das Suchfenster, das zum Anzeigen der Gruppen verwendet wird.

Gruppenlistenfenster

Definiert das Fenster, welches die Spalten und die Sortierung auf dieser Registerkarte bestimmt.

Admin-Rollen-Suchfenster

Definiert das Suchfenster, das zum Anzeigen der Admin-Rollen verwendet wird.

Admin-Rollen-Listenfenster

Definiert das Fenster, welches die Spalten und die Sortierung auf dieser Registerkarte bestimmt.

Admin-Aufgaben-Suchfenster

Definiert das Suchfenster, das zum Anzeigen der Admin-Aufgaben verwendet wird.

Admin-Aufgaben-Listenfenster

Definiert das Fenster, welches die Spalten und die Sortierung auf dieser Registerkarte bestimmt.

Online-Anfragen

Mit CA IdentityMinder können Sie Aufgaben für Online-Anfragen erstellen, die für allgemeine Zwecke verfügbar sind. Die standardmäßige Implementierung von Online-Anfragen besteht aus einem Satz zugehöriger Aufgaben für selbständernde Anfragen und administrative Änderungsanfragen durch Benutzer. Die Funktion für Online-Anfragen kann jedoch problemlos für andere Anfrageaufgaben von CA IdentityMinder implementiert werden.

Eine Benutzeränderungsanfrage löst einen Workflow-Prozess aus, der ein Arbeitselement generiert. Workflow-Teilnehmer können das Arbeitselement entweder genehmigen und implementieren oder ablehnen. Der Benutzer, der die Aufgabe initiiert, gibt im Verlaufseditor eine Beschreibung der Anfrage ein. CA IdentityMinder verwendet dieses Textfeld, um den Verlauf einer Anfrage zu verwalten. Dieser Verlaufseditor kann so konfiguriert werden, dass er Teilnehmern das Hinzufügen von Kommentaren zu den von ihnen durchgeführten Aktionen für das Arbeitselement gestattet. Diese Kommentare werden zu Bestandteilen des kumulativen Arbeitselementverlaufs.

Es sind auch neue Aktionen möglich, die zusätzlich zu den (oder anstelle der) standardmäßigen Genehmigungs- und Ablehnungsaktionen hinzugefügt werden. Beispiel: Ein Business-Teilnehmer kann eine Anfrage spezifizieren oder kommentieren und ein technischer Teilnehmer kann die Anfrage implementieren. Diese neuen Aktivitäten können durch neue Workflow-Aktionsschaltflächen dargestellt werden, wie "Spezifizieren" und "Implementieren", die Sie für die Genehmigungsaufgabe zu den Standardschaltflächen "Genehmigen" und "Ablehnen" hinzufügen können.

Online-Anfrage-Aufgaben

Es gibt fünf Aufgaben, die zusammenarbeiten, um die standardmäßige Implementierung von Online-Anfragen zu bilden. Diese Aufgaben zeigen die Verwendung der Schaltflächen für benutzerdefinierte Anfragen, Verlauf und Workflow-Aktionen:

Hinweis: Die Admin-Aufgaben ("Mein Konto ändern" und "Online-Anfrage erstellen") sind standardmäßig für ereignisbezogenen Workflow konfiguriert und verwenden die Vorlage für den Rückspracheprozess.

Mein Konto ändern

Dies ist eine selbständernde Admin-Aufgabe, die eine Änderungsanfrage für ein Benutzerkonto erstellt. Sie hat eine Registerkarte "Anfrage" mit einem Verlaufseditor für die Beschreibung der Anfrage und eine Registerkarte "Profil", mit schreibgeschützten Benutzerangaben.

Online-Anfrage erstellen

Dies ist eine Admin-Aufgabe für eine Änderung durch den Benutzer, die eine Kontoänderungsanfrage für einen bestimmten Benutzer erstellt. Sie hat eine Registerkarte "Anfrage" mit einem Verlaufseditor für die Beschreibung der Anfrage und eine Registerkarte "Subjektprofil", mit schreibgeschützten Benutzerangaben.

Online-Anfrage genehmigen

Dies ist eine Genehmigungsaufgabe, die es dem Business-Teilnehmer ermöglicht, die Aufgabe zu genehmigen oder abzulehnen oder eine weitere Spezifizierung der Aufgabe anzufordern. Diese Aufgabe hat eine Registerkarte "Anfrage" mit einer Verlaufsanzeige sowie einen Verlaufseditor für Abfragen und Kommentare, eine schreibgeschützte Registerkarte "Subjektprofil" und eine Registerkarte "Bevollmächtigte".

Online-Anfrage spezifizieren

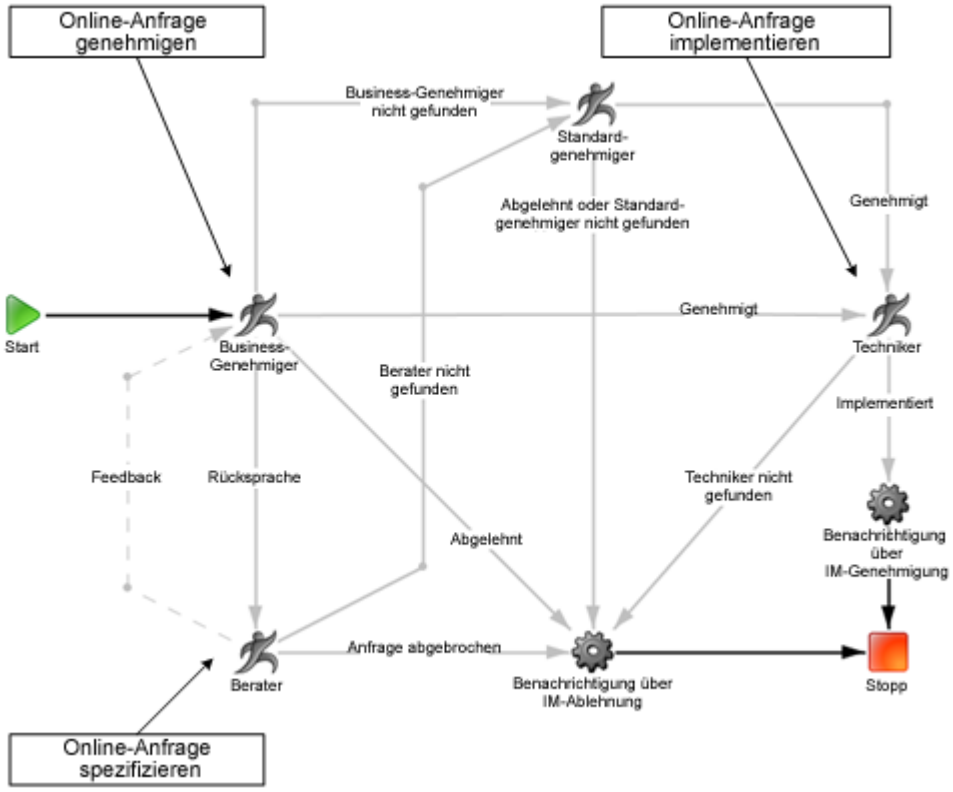
Dies ist eine Genehmigungsaufgabe, die es dem spezifizierenden Teilnehmer ermöglicht, auf eine Spezifizierungsanfrage zu antworten. Anschließend sendet sie die Aufgabe zur Genehmigung zurück an den Business-Teilnehmer. Sie hat eine Registerkarte "Anfrage" mit einer Verlaufsanzeige und einem Verlaufseditor für Kommentare sowie eine schreibgeschützte Registerkarte "Subjektprofil".

Online-Anfrage implementieren

Dies ist eine Genehmigungsaufgabe mit der der technische Teilnehmer die Aufgabe implementieren und einen Kommentar zum Aufgabenverlauf hinzufügen kann. Sie hat eine Registerkarte "Anfrage implementieren" mit einer Verlaufsanzeige und einem Verlaufseditor für Kommentare, eine schreibgeschützte Registerkarte "Subjektprofil" und eine Registerkarte "Bevollmächtigte".

Online-Anfrageprozess

Die Aufgaben für Online-Anfragen werden durch eine Workflow-Prozessvorlage namens Rückspracheprozess kontrolliert, die wie folgt in WorkPoint Designer angezeigt wird:



Der Rückspracheprozess umfasst vier manuelle Aktivitäten, die Genehmigungsaufgaben in der Online-Anfrage-Implementierung entsprechen:

- Eine Aktivität für den Business-Genehmiger, die das Arbeitselement ablehnt, der das Arbeitselement genehmigt und an den Techniker übergibt oder eine weitere Spezifizierung vom Berater anfordert.
- Eine Aktivität für den Berater, der das Arbeitselement spezifiziert und zurück an den Business-Genehmiger sendet.
- Eine Aktivität für einen Standardgenehmiger, der übernimmt, wenn Business-Genehmiger oder Berater nicht erreicht werden können.
- Eine Aktivität für den Techniker, der die Anfrage implementiert und das Arbeitselement abschließt.

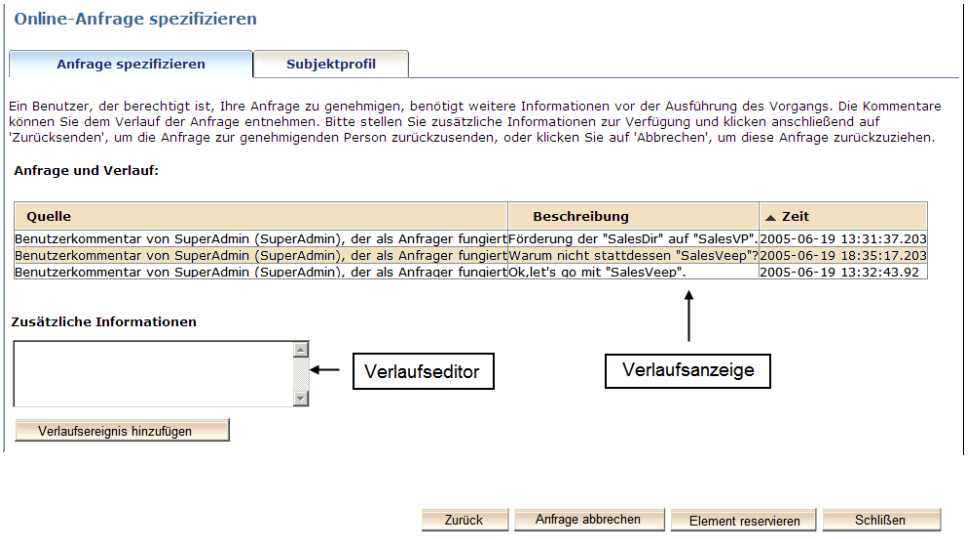
Verlauf der Online-Anfrage

Mit der Funktion für den Verlauf der Online-Anfrage können Teilnehmer eine Aufzeichnung von Arbeitselementaktionen erstellen. Wenn die Verantwortung für das Arbeitselement von einem Teilnehmer an einen anderen übergeht, kann der neue Teilnehmer den Verlauf des Arbeitselements prüfen, bevor er eine Aktion einleitet.

Zur Implementierung des Verlaufs der Online-Anfrage werden zwei Steuerelemente verwendet:

- Bei der Verlaufsanzeige handelt es sich um eine schreibgeschützte Tabelle mit Details der bisherigen Verlaufseinträge in chronologischer Reihenfolge.
- Der Verlaufseditor ist ein Textfeld, in dem neue Einträge erstellt werden. Er besitzt eine optionale Schaltfläche zum Hinzufügen mehrer Einträge, ohne das Arbeitselement zu übermitteln.

Standardmäßig erscheinen der Verlaufseditor und die Verlaufsanzeige für alle der Online-Anfrage-Implementierung zugeordneten Aufgaben auf der Registerkarte "Anfrage". Das folgende Fenster zeigt die Verlaufssteuerelemente in der Aufgabe "Online-Anfrage spezifizieren":


Online-Anfrage spezifizieren
Anfrage spezifizieren
Subjektprofil
Ein Benutzer, der berechtigt ist, Ihre Anfrage zu genehmigen, benötigt weitere Informationen vor der Ausführung des Vorgangs. Die Kommentare können Sie dem Verlauf der Anfrage entnehmen. Bitte stellen Sie zusätzliche Informationen zur Verfügung und klicken anschließend auf 'Zurücksenden', um die Anfrage zur genehmigenden Person zurückzusenden, oder klicken Sie auf 'Abbrechen', um diese Anfrage zurückzuziehen.
Anfrage und Verlauf:
Quelle
Beschreibung
Zeit
Benutzerkommentar von SuperAdmin (SuperAdmin), der als Anfrager fungiert
Förderung der "SalesDir" auf "SalesVP".
2005-06-19 13:31:37.203
Benutzerkommentar von SuperAdmin (SuperAdmin), der als Anfrager fungiert
Warum nicht stattdessen "SalesVeep"?
2005-06-19 18:35:17.203
Benutzerkommentar von SuperAdmin (SuperAdmin), der als Anfrager fungiert
Ok,let's go mit "SalesVeep".
2005-06-19 13:32:43.92
Zusätzliche Informationen
Verlaufseditor
Verlaufsanzeige
Verlaufsereignis hinzufügen
Zurück
Anfrage abbrechen
Element reservieren
Schließen

Verwenden von Online-Anfragen

Die folgenden Schritte beschreiben den Workflow-Prozess einer Online-Anfrage. Für jeden Schritt wird in Klammern die generierte IM-Aufgabe angezeigt. Innerhalb jedes Schrittes kann der Teilnehmer im Verlaufseditor einen Kommentar hinzufügen. Dieser Kommentar erscheint in der Verlaufsanzeige für den nächsten Teilnehmer im Workflow-Prozess.

1. Der Aufgabeninitiator fordert von einem IM-Benutzer eine Änderung an (Online-Anfrage erstellen).
2. Der Business-Genehmiger empfängt ein Arbeitselement und führt eine der folgenden Aktionen durch:
   - Genehmigt das Arbeitselement (Online-Anfrage genehmigen).
   - Lehnt das Arbeitselement ab und beendet den Workflow-Prozess. Es wird keine neue Aufgabe erzeugt.
   - Anfragen zur Spezifizierung durch den Berater (Online-Anfrage spezifizieren).
3. Der Berater empfängt ein Arbeitselement und führt eine der folgenden Aktionen durch:
   - Fügt eine Spezifizierung hinzu und sendet das Arbeitselement zurück an den Business-Genehmiger. Es wird keine neue Aufgabe erzeugt.
   - Bricht das Arbeitselement ab und beendet den Workflow-Prozess. Es wird keine neue Aufgabe erzeugt.
4. Der Techniker empfängt ein Arbeitselement und implementiert die Anfrage (Online-Anfrage implementieren).

Schaltflächen für Workflow-Aktionen

Genehmigungsaufgaben in CA IdentityMinder verfügen über die Aktionsschaltflächen "Genehmigen" und "Ablehnen", die auf den entsprechenden Arbeitselementfenstern angezeigt werden. Workflow-Aktionsschaltflächen ermöglichen es Administratoren, die Funktion von CA IdentityMinder-Aufgaben und -Workflows zu erweitern, indem Aktionsschaltflächen zu Genehmigungsaufgaben hinzugefügt werden und indem vorhandene Schaltflächen entfernt oder geändert werden. (Die standardmäßigen Schaltflächen "Genehmigen" und "Ablehnen" werden auf gleiche Weise implementiert wie die benutzerdefinierten Workflow-Aktionsschaltflächen.)

Zum Beispiel könnte für einen Workflow-Prozess eine Aktion erforderlich sein, mit der ein Teilnehmer auf mittlerer Ebene bestimmte Fälle zu einem älteren Teilnehmer zur letzten Genehmigung oder Ablehnung eskalieren kann. Diese Teilnehmer auf mittlerer Ebene können einen Kommentar oder eine Empfehlung mithilfe des Verlaufseditors hinzufügen, und das Arbeitselement kann an den älteren Teilnehmer zur Überprüfung gesendet werden, der das Arbeitselement dann genehmigt oder ablehnt.

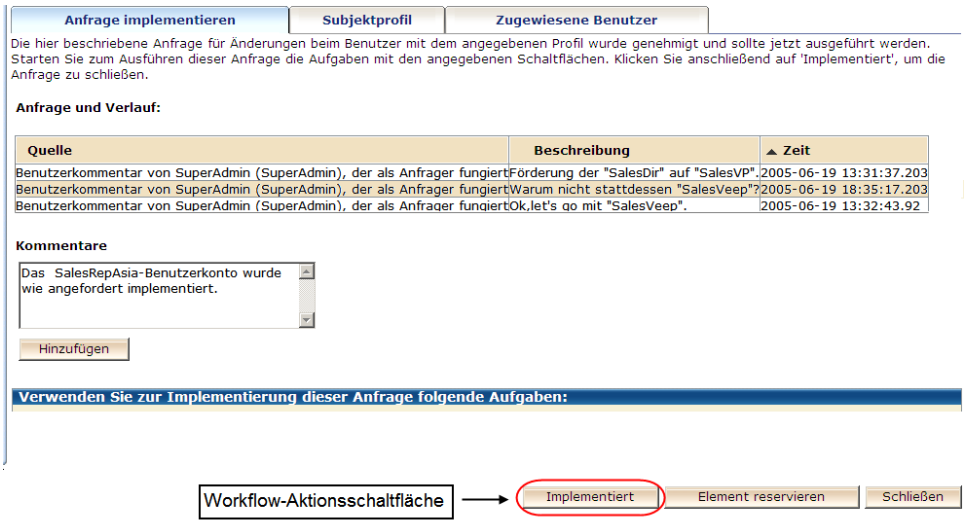
Das Hinzufügen oder Entfernen von Workflow-Aktionsschaltflächen erfordert Änderungen am WorkPoint-Workflow-Prozess, der die Business-Logik für die Verarbeitung dieser neuen Aktionen bereitstellt.

Weitere Informationen:

Schaltflächenkonfiguration in CA IdentityMinder (siehe Seite 367)
Workflow-Schaltflächen in Genehmigungsaufgaben (siehe Seite 367)
Schaltflächenkonfiguration in WorkPoint Designer (siehe Seite 370)

Workflow-Schaltflächen in Genehmigungsaufgaben

Workflow-Aktionsschaltflächen entsprechen Transitionsknoten, die in einem WorkPoint-Prozessdiagramm von manuellen Knoten abgehen. Beispiel: Im Rückspracheprozess besitzt der Aktivitätsknoten "Techniker" eine einzige Transition "Implementiert". Diese entspricht der Schaltfläche "Implementiert" innerhalb der Aufgabe "Online-Anfrage implementieren", was die folgende Abbildung zeigt:


Anfrage implementieren
Subjektprofil
Zugewiesene Benutzer
Die hier beschriebene Anfrage für Änderungen beim Benutzer mit dem angegebenen Profil wurde genehmigt und sollte jetzt ausgeführt werden. Starten Sie zum Ausführen dieser Anfrage die Aufgaben mit den angegebenen Schaltflächen. Klicken Sie anschließend auf 'Implementiert', um die Anfrage zu schließen.
Anfrage und Verlauf:
Quelle
Beschreibung
Zeit
Benutzerkommentar von SuperAdmin (SuperAdmin), der als Anfrager fungiert
Förderung der "SalesDir" auf "SalesVP".
2005-06-19 13:31:37.203
Benutzerkommentar von SuperAdmin (SuperAdmin), der als Anfrager fungiert
Warum nicht stattdessen "SalesVeep"?
2005-06-19 18:35:17.203
Benutzerkommentar von SuperAdmin (SuperAdmin), der als Anfrager fungiert
Ok,let's go mit "SalesVeep".
2005-06-19 13:32:43.92
Kommentare
Das SalesRepAsia-Benutzerkonto wurde wie angefordert implementiert.
Hinzufügen
Verwenden Sie zur Implementierung dieser Anfrage folgende Aufgaben:
Workflow-Aktionsschaltfläche
Implementiert
Element reservieren
Schließen

Hinweis: Die Schaltflächen "Element reservieren" und "Schließen" werden durch die Programmlogik von CA IdentityMinder gesteuert und befinden sich nicht unter Workflow-Kontrolle.

Weitere Informationen:

Schaltflächen für Workflow-Aktionen (siehe Seite 366)
Schaltflächenkonfiguration in CA IdentityMinder (siehe Seite 367)

Schaltflächenkonfiguration in CA IdentityMinder

Zum Konfigurieren einer Workflow-Aktionsschaltfläche klicken Sie auf der Registerkarte "Profil" auf die Schaltfläche namens "Workflow-Aktionsschaltflächen".

Die Registerkarte für das Schaltflächenprofil zeigt eine Tabelle, in der in jeder Zeile eine Workflow-Aktionsschaltfläche angegeben ist. Alle Schaltflächenzeilen besitzen die folgenden vier Eigenschaften, die den Spalten der Tabelle entsprechen:

Anzeigename

Der Name, der im Genehmigungsfenster auf der Schaltfläche erscheint. Der Name ist ein bedingt lokalisierter Wert, bei dem es sich entweder um eine Zeichenfolge oder um einen Schlüssel für eine lokalisierte Zeichenfolge in einer Ressourcendatei handeln kann.

Aktion

Der an den Workflow-Prozess zurückgegebene Wert, wenn die Option aktiviert ist. Dieser Wert ist ein Attribut des entsprechenden Transitionsknotens im WorkPoint-Prozessdiagramm. Der Wert ist eine nicht lokalisierte Zeichenfolge. Die Standardeinstellungen sind "Genehmigt" und "Abgelehnt".

Quickinfo

Eine kurze Beschreibung (oder ein Quickinfo) der Schaltflächenaktion, die angezeigt wird, wenn der Benutzer den Mauszeiger über die Schaltfläche führt. Der Name ist ein bedingt lokalisierter Wert, bei dem es sich entweder um eine Zeichenfolge oder um einen Schlüssel für eine lokalisierte Zeichenfolge in einer Ressourcendatei handeln kann.

Ausführliche Beschreibung

Eine längere Beschreibung der Schaltflächenaktion, die eine Nachricht hinzufügt, mit der die Aktion im Fenster "Gesendete Aufgaben anzeigen" beschrieben wird. Wenn die Beschreibung leer ist, ist die Meldung im Fenster "Gesendete Aufgaben anzeigen" der Schaltflächenname. Der Name ist ein bedingt lokalisierter Wert, bei dem es sich entweder um eine Zeichenfolge oder um einen Schlüssel für eine lokalisierte Zeichenfolge in einer Ressourcendatei handeln kann.

Weitere Informationen:

Schaltflächenkonfiguration in WorkPoint Designer (siehe Seite 370)

Hinzufügen von Workflow-Aktionsschaltflächen

Folgende grundlegende Schritte sind erforderlich, um eine neue Schaltfläche zu einem vorhandenen Workflow-Prozess hinzuzufügen:

1. Fügen Sie in Identity Manager die folgende Workflow-Schaltfläche hinzu.

   Eine Anleitung finden Sie unter So fügen Sie eine Workflow-Aktionsschaltfläche hinzu (siehe Seite 369).

2. Fügen Sie gegebenenfalls Lokalisierungsschlüssel hinzu.

   Eine Anleitung finden Sie im *Konfigurationshandbuch*.

3. Fügen Sie alle erforderlichen neuen Knoten in WorkPoint Designer hinzu

   Eine Anleitung finden Sie in der Online-Hilfe für WorkPoint Designer

4. Definieren Sie im WorkPoint Designer-Transitionsknoten ein Skript.

   Eine Anleitung finden Sie unter Schaltflächenkonfiguration in WorkPoint Designer (siehe Seite 370).

Weitere Informationen:

Schaltflächenkonfiguration in WorkPoint Designer (siehe Seite 370)
So fügen Sie eine Workflow-Aktionsschaltfläche hinzu: (siehe Seite 369)

So fügen Sie eine Workflow-Aktionsschaltfläche hinzu:

Sie können Genehmigungsaufgaben in CA IdentityMinder Workflow-Aktionsschaltflächen hinzufügen.

So fügen Sie eine Workflow-Aktionsschaltfläche zu einer Admin-Aufgabe hinzu:

1. Wählen Sie in der Benutzerkonsole die Optionen "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe ändern" aus.

   Das Fenster "Admin-Aufgabe auswählen" wird geöffnet.

2. Suchen Sie nach der Genehmigungsaufgabe, und klicken Sie auf "Auswählen".

   Das Fenster "Admin-Aufgabe ändern" wird geöffnet.

3. Klicken Sie auf der Registerkarte "Profil" auf die Schaltfläche "Workflow-Aktionsschaltflächen".

   Die Registerkarte "Workflow-Aktionsschaltflächenprofil" wird angezeigt.

4. Klicken Sie auf "Schaltfläche hinzufügen", um der Genehmigungsaufgabe eine neue Schaltfläche hinzuzufügen.

5. Geben Sie die Informationen für die Schaltflächeneigenschaft ein.

6. Klicken Sie auf "OK".

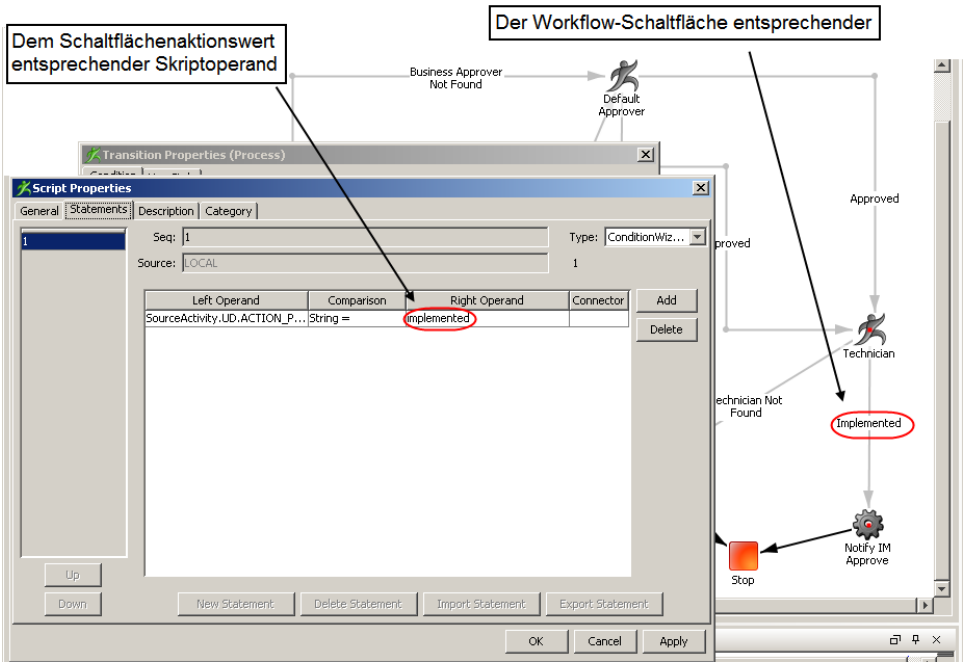
   CA IdentityMinder speichert die neuen Schaltflächeninformationen.

7. Klicken Sie auf "Senden".

   CA IdentityMinder verarbeitet die Aufgabenänderung.

Schaltflächenkonfiguration in WorkPoint Designer

In WorkPoint Designer werden Workflow-Aktionsschaltflächen mit Hilfe von Transitionsknotenskripteigenschaften konfiguriert, wie in der folgenden Abbildung zu sehen ist:



Standardmäßig verwenden Workflow-Aktionsschaltflächen die folgenden Skripteigenschaften, um Zeichenketten zu vergleichen:

- Linker Operand: ACTION_PEFORMED, der in den Benutzerdateneigenschaften des vorangehenden manuellen Aktivitätsknotens definiert ist.
- Rechter Operand: Der Aktionswert der Schaltfläche, der auf der Registerkarte "Schaltflächenprofil" in der Benutzerkonsole definiert ist.

Hinweis: In der Online-Hilfe zu WorkPoint Designer finden Sie Informationen zu Skripts für und Eigenschaften von Aktivitäts- und Transitionsknoten.

Weitere Informationen:

Schaltflächenkonfiguration in CA IdentityMinder (siehe Seite 367)

Arbeitslisten und Arbeitselemente

Eine *Arbeitsliste* ist eine Liste von Arbeitselementen (oder Genehmigungsaufgaben), die in der Benutzerkonsole des Teilnehmers angezeigt wird, der berechtigt ist, die Aufgabe zu genehmigen. Arbeitselemente entsprechen manuellen Aktivitäten in einem Workflow-Prozess. Arbeitselemente werden als Zeilen in der Arbeitsliste dargestellt.

Arbeitselemente können auf folgende Weise in eine Arbeitsliste eingefügt werden:

- Ein Resolver für Teilnehmer bestimmt eine Liste von Genehmigern.
- Sie erhalten delegierte Arbeitselemente von einem anderen Benutzer.
- Neu zuweisen an einen anderen Benutzer.

Arbeitselemente können auf folgende Weise aus einer Arbeitsliste entfernt werden:

- Abschließen (Genehmigen oder Ablehnen) des Arbeitselements.
- Neu zuweisen an einen anderen Benutzer.
- Reservieren. Dadurch wird das Arbeitselement aus den Arbeitslisten aller anderen Teilnehmer gelöscht.

Hinweis: Wenn Sie ein Arbeitselement annehmen oder ablehnen, wird die Änderung nicht sofort angezeigt. Wenn Sie beispielsweise ein Arbeitselement ablehnen, wird das Element weiterhin in Ihrer Arbeitsliste angezeigt, bis der Workflow-Prozess die Informationen speichert und den Prozess in den nächsten Knoten überführt.

Welche Informationsregisterkarten für ein Arbeitselement angezeigt werden, hängt davon ab, ob das Arbeitselement durch Workflow unter aufgaben- oder ereignisbezogener Kontrolle generiert wurde:

- **Profil**: Liefert Profilinformationen zum Objekt, das vom Ereignis betroffen ist (nur ereignisbezogen).
- **Aufgabendetails**: Bietet detaillierte Informationen zu allen Ereignissen innerhalb einer Aufgabe (nur aufgabenbezogen).
- **Genehmiger**: Liste aller einzelnen Genehmiger und Delegierenden für die Aufgabe oder das Ereignis (aufgabenbezogen und ereignisbezogen)

Anzeigen einer Arbeitsliste

Ihre Arbeitsliste erscheint automatisch, wenn Sie sich bei der Benutzerkonsole anmelden, sofern Sie als Teilnehmer für Genehmigungsaufgaben (oder Arbeitselemente), die von anderen Benutzern initiiert wurden, festgelegt wurden.

So zeigen Sie Ihre Arbeitsliste manuell an

1. Wählen Sie in der Benutzerkonsole "Startseite", "Meine Arbeitsliste anzeigen" aus.

   Ihre Arbeitsliste wird angezeigt.

2. Klicken Sie auf den Namen eines Arbeitselements, damit es angezeigt wird.

   Das ausgewählte Arbeitselement wird angezeigt.

Administratoren können Arbeitselemente für Benutzer verwalten, die zu ihrem Bereich gehören.

Hinweis: Bei der Verwaltung der Arbeitselemente eines Benutzers kann der Administrator ein Arbeitselement reservieren. Das Anzeigen der Arbeitsliste eines Benutzer erlaubt keinerlei Änderungen von Arbeitselementen.

So zeigen Sie die Arbeitsliste eines anderen Benutzers an

1. Wählen Sie in der Benutzerkonsole "Benutzer", "Arbeitselemente verwalten", "Arbeitsliste des Benutzers anzeigen" aus.

   Ein Fenster für die Auswahl des Benutzers wird geöffnet.

2. Suchen Sie den Benutzer, dessen Arbeitsliste Sie anzeigen möchten, und klicken Sie auf "Auswählen".

   Das Fenster mit der Arbeitsliste des Benutzers wird geöffnet.

So verwalten Sie Arbeitselemente für einen anderen Benutzer:

1. Wählen Sie in der Benutzerkonsole "Benutzer", "Arbeitselemente verwalten", "Arbeitselemente des Benutzers verwalten" aus.

   Ein Fenster für die Auswahl des Benutzers wird geöffnet.

2. Suchen Sie den Benutzer, dessen Arbeitselemente Sie verwalten möchten, und klicken Sie auf "Auswählen".

   Das Fenster mit der Arbeitsliste des Benutzers wird geöffnet.

3. Klicken Sie auf den Namen eines Arbeitselements, damit es angezeigt wird.

   Das ausgewählte Arbeitselement wird angezeigt.

Reservieren von Arbeitselementen

Sie können ein Arbeitselement reservieren, um es "auszuchecken" und aus den Arbeitslisten anderer Teilnehmer zu entfernen. Das Reservieren eines Arbeitselements bringt es in den Besitz des Benutzers, der die Reservierung durchführt.

Wenn der reservierende Benutzer das Arbeitselement freigibt, wird es erneut in den Arbeitslisten der anderen Teilnehmer verfügbar. Wenn der reservierende Benutzer das Arbeitselement genehmigt oder ablehnt, ist es abgeschlossen und nicht mehr für andere Teilnehmer verfügbar.

Weitere Informationen:

Delegierung und reservierte Arbeitselemente (siehe Seite 373)
Neue Zuweisung und reservierte Arbeitselemente (siehe Seite 373)

Neue Zuweisung und reservierte Arbeitselemente

Wenn ein Benutzer ein Arbeitselement reserviert hat, während es neu zugewiesen wird, bleibt es für den Benutzer reserviert. Sobald der Benutzer das Arbeitselement dann aber freigibt, verliert er den Zugriff darauf.

Ein Administrator kann die Arbeitselemente eines anderen Benutzers neu zuweisen, reservieren oder freigeben, er kann ein Arbeitselement eines anderen Benutzers aber weder genehmigen noch ablehnen. Dies kann ausschließlich der dem Arbeitselement zugewiesene Teilnehmer.

Weitere Informationen:

Neuzuweisen von Arbeitselementen (siehe Seite 380)

Delegierung und reservierte Arbeitselemente

Während eine Delegierung aktiv ist, können entweder der Stellvertreter oder der Delegierende ein Arbeitselement reservieren. Ein von einem Benutzer reserviertes Arbeitselement kann nicht in der Arbeitsliste eines anderen Benutzers erscheinen.

Wenn z. B. ein Stellvertreter ein Arbeitselement reserviert hat, während die Delegierung zurückgenommen wird, bleibt das Arbeitselement für den Stellvertreter reserviert. Sobald der Stellvertreter das Arbeitselement dann aber freigibt, verliert er den Zugriff darauf.

Wenn ein Benutzer, der Stellvertreter ist, gelöscht wird, während er ein Arbeitselement reserviert hat, bleibt das Arbeitselement weiterhin beim Stellvertreter. Wenn der Stellvertreter das Arbeitselement dann genehmigt, kann das Auditing nicht mehr ermitteln, wer es delegiert hat.

Wenn ein Stellvertreter ein Arbeitselement reserviert hat, während die Delegierung zurückgenommen wird, bleibt der Zugriff so lange beim Stellvertreter bis das Arbeitselement abgeschlossen oder freigegeben wird.

Weitere Informationen:

Delegieren von Arbeitselementen (siehe Seite 374)
Reservieren von Arbeitselementen (siehe Seite 373)

So reservieren Sie ein Arbeitselement und geben es wieder frei:

Sie können ein Arbeitselement reservieren, um es "auszuchecken" und aus den Arbeitslisten anderer Teilnehmer zu entfernen.

Sie können das reservierte Arbeitselement freigeben, um es wieder in den Arbeitslisten der anderen Teilnehmer verfügbar zu machen.

Hinweis: Ein reserviertes Arbeitselement kann nur wieder verfügbar gemacht werden, indem es explizit freigegeben wird.

So reservieren Sie ein Arbeitselement und geben es wieder frei:

1. Wählen Sie in der Benutzerkonsole "Startseite", "Meine Arbeitsliste anzeigen" aus.

   Ihre Arbeitsliste wird angezeigt.

2. Wählen Sie das Arbeitselement aus, das Sie reservieren oder freigeben möchten.

   Das erweiterte Arbeitselementfenster wird geöffnet.

3. Klicken Sie auf "Element reservieren" oder auf "Element freigeben".

   CA IdentityMinder bestätigt Ihre Aktion.

Delegieren von Arbeitselementen

Beim *Delegieren* von Arbeitselementen legt ein Benutzer (der Delegierende) fest, dass ein anderer Benutzer (der Stellvertreter) berechtigt ist, Aufgaben in der Arbeitsliste des Delegierenden zu genehmigen. Ein Delegierender kann für Zeiträume, in denen der Delegierende außer Haus, ist Arbeitselemente einem anderen Genehmiger zuweisen. Stellvertreter haben während des Delegierungszeitraums vollen Zugriff auf ihre Arbeitselemente.

Delegierte Arbeitselemente werden nicht verändert. Die Protokollierung zeigt an, ob ein Arbeitselement delegiert wurde.

Die Delegierung erlaubt dem Stellvertreter sich sozusagen als der Delegierende "auszugeben" und die Elemente der Arbeitsliste des Delegierenden anzusehen. Beim Anzeigen einer Arbeitsliste sehen Stellvertreter ihre eigenen Arbeitselemente sowie die Arbeitselemente des Delegierenden.

Die Delegierung ist nicht transitiv. Ein Stellvertreter kann nur die Arbeitselemente sehen, die der Delegierende direkt zugewiesen hat. Beispiel: Wenn Benutzer A Arbeitselemente an Benutzer B delegiert und Benutzer B delegiert Arbeitselemente an Benutzer C, kann Benutzer C nur Arbeitselemente sehen, die Benutzer B gehören. Arbeitselemente, die durch Benutzer A an Benutzer B delegiert wurden, sieht er nicht.

Weitere Informationen:

Delegierung und reservierte Arbeitselemente (siehe Seite 373)

Bekanntes Attribut der Delegierung

Die Delegierung verwendet das folgende bekannte Attribut:

%DELEGATORS%

Dieses bekannte Attribut speichert die Namen der Benutzer, die eine Delegierung an den Benutzer mit dem Attribut vornehmen sowie den Zeitpunkt der Erstellung der Delegierung.

Aktivieren der Delegierung

Die Workflow-Genehmigungsdelegierung muss aktiviert sein, bevor Sie die delegierten Arbeitselemente eines anderen Benutzers verwenden können. Die Delegierung ist standardmäßig deaktiviert.

So aktivieren Sie die Delegierung der Workflow-Genehmigung

1. Öffnen Sie die Management-Konsole, indem Sie die folgende URL in einen Browser eingeben:

   `http://hostname/iam/immanage`

   Hostname

   Definiert dem voll qualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist. Beispiel: myserver.mycompany.com:port.

2. Klicken Sie auf "Umgebungen" und wählen Sie anschließend den Namen der jeweiligen CA IdentityMinder-Umgebung aus.

3. Klicken Sie auf "Erweiterte Einstellungen" und anschließend auf "Delegierung der Workflow-Genehmigung".
4. Aktivieren Sie das Kontrollkästchen "Aktiviert", und klicken Sie auf "Speichern".

Weitere Informationen:

So führen Sie eine Delegierung für sich selbst durch: (siehe Seite 376)
So führen Sie eine Delegierung für einen anderen Benutzer durch (siehe Seite 379)

So führen Sie eine Delegierung für sich selbst durch:

Sie können Arbeitselemente für Zeiträume, in denen Sie außer Haus sind, an andere Benutzer delegieren. Delegierende haben während des Delegierungszeitraums weiterhin vollen Zugriff auf ihre Arbeitselemente.

So delegieren Sie Arbeitselemente für sich selbst:

1. Wählen Sie in der Benutzerkonsole "Startseite", "Abwesenheits-Assistent" aus.

   Das Fenster "Abwesenheits-Assistent" wird geöffnet.
2. Klicken Sie auf "Benutzer hinzufügen".

   Ein Fenster für die Auswahl des Benutzers wird geöffnet.
3. Suchen Sie einen oder mehrere Benutzer, die als Stellvertreter agieren sollen.

   Die Benutzer werden zur Stellvertreterliste hinzugefügt.
4. Klicken Sie auf "Senden".

   Die Aufgabe wird gesendet und die Delegierung gespeichert.

Hinweis: Benutzer, die bereits Stellvertreter sind, erscheinen beim Hinzufügen eines Stellvertreters nicht in den Suchergebnissen.

Weitere Informationen:

Aktivieren der Delegierung (siehe Seite 375)

Zeitbasierte Delegierung von Arbeitselementen

In früheren Versionen konnte die Startzeit, jedoch nicht die Endzeit für Delegierungen angegeben werden. Bei neu erstellten Delegierungen werden die Daten für die Delegierung auf "True" (Wahr) gesetzt, und für die Standard-Startzeit wird "Jetzt" festgelegt.

Zum Zeitpunkt der Änderung können Start- und Enddatum geändert werden. Die Standard-Endzeit ist eine Woche nach dem Startdatum.

Sie können das Start- oder Enddatum ändern, indem Sie die folgenden Schritte ausführen:

1. Wählen Sie auf der Registerkarte "Startseite" der Benutzerkonsole "Abwesenheits-Assistent" aus.
2. Klicken Sie auf das Stift-Symbol neben der Benutzer-ID, deren Delegierungsinformationen Sie ändern möchten.

   Das Fenster "Delegierungsdetails bearbeiten" wird angezeigt.
3. Klicken Sie auf den Kalender neben "Startdatum", um das Startdatum der Delegierung zu ändern.

   Hinweis: Wenn für die Delegierung ein Startdatum ausgewählt wird, das vor dem aktuellen Datum liegt, wird eine Fehlermeldung angezeigt.
4. Wenn Sie ein Enddatum auswählen möchten, aktivieren Sie das Kontrollkästchen "Hat Enddatum".

   Das Feld "Enddatum" ist nun zum Festlegen des Enddatums verfügbar.
5. Klicken Sie auf den Kalender neben "Enddatum", um ein Enddatum für die Delegierung festzulegen.
6. Wenn Sie die Daten festgelegt haben, klicken Sie auf "OK".

Alternativ können Sie denselben Vorgang bei der Erstellung oder Änderung eines Benutzers über die Registerkarte "Arbeitselemente delegieren" ausführen.

Aktivieren der zeitbasierten Delegierung von Arbeitselementen

Führen Sie die folgenden Schritte aus, um die zeitbasierte Delegierung von Arbeitselementen in einer vorhandenen Umgebung bei einem Upgrade zu aktivieren:

Über die Managementkonsole

1. Navigieren Sie zur Seite "Umgebungen".
2. Wählen Sie die ausgewählte Umgebung, "Erweiterte Einstellungen", "Arbeitselemente delegieren".
3. Deaktivieren Sie das Kontrollkästchen "Aktiviert".
4. Speichern Sie die Änderungen und starten Sie die Umgebung neu.
5. Wählen Sie "Erweiterte Einstellungen", "Arbeitselemente delegieren".
6. Aktivieren Sie das Kontrollkästchen "Aktiviert".
7. Speichern Sie die Änderungen und starten Sie die Umgebung neu.

Hinweis: Dieser Vorgang bezieht sich nur auf vorhandene Umgebungen. Für neue Umgebungen ist die zeitbasierte Delegierung von Workflow-Elementen aktiviert.

Fenster des Abwesenheits-Assistenten

Im folgenden Fenster des Abwesenheits-Assistenten können Sie Ihre Stellvertreter hinzufügen oder löschen:

Das Fenster des Abwesenheits-Assistenten enthält eine Liste Ihrer aktuellen Stellvertreter. Neben der Spalte mit den Stellvertretern enthält die Liste drei weitere Spalten:

Startdatum

Zeigt das Datum an, an dem die Delegierung erstellt wurde.

Enddatum

Zeigt das Enddatum der Delegierung an.

Hat Delegierte

Zeigt an, ob der Stellvertreter Arbeitselemente an einen anderen Benutzer delegiert hat.

Wenn Sie auf das Stift-Symbol neben der ausgewählten Benutzer-ID klicken, wird das Fenster "Delegierungsdetails bearbeiten" angezeigt, in dem Sie das Startdatum ändern und das Enddatum für die Delegierung angeben können.

So führen Sie eine Delegierung für einen anderen Benutzer durch

Administratoren können Arbeitselemente von einem Benutzer (dem Delegierenden) an einen anderen delegieren. Beispiel: Ein Benutzer ist unerwartet außer Haus oder ein Administrator muss eine umfangreiche Arbeit mehreren Benutzern zuordnen.

Administratoren können nur Arbeitselemente für Benutzer delegieren, die zu ihrem Bereich gehören. Entsprechend können Sie nur von ihnen verwaltete Benutzer zur Liste der Stellvertreter hinzufügen oder daraus entfernen.

So delegieren Sie Arbeitselemente für einen anderen Benutzer:

1. Wählen Sie in der Benutzerkonsole "Benutzer", "Arbeitselemente verwalten", "Arbeitselemente delegieren" aus.

   Ein Fenster für die Auswahl des Benutzers wird geöffnet.

2. Suchen Sie den Benutzer, dessen Arbeitselemente Sie delegieren möchten (den Delegierenden), und klicken Sie auf "Auswählen".

   Ein Fenster zum Delegieren von Arbeitselementen wird geöffnet.

3. Klicken Sie auf "Benutzer hinzufügen".

   Ein Fenster für die Auswahl des Benutzers wird geöffnet.

4. Suchen Sie einen oder mehrere Benutzer, die als Stellvertreter agieren sollen.

   Die Benutzer werden zur Stellvertreterliste hinzugefügt.

5. Klicken Sie auf "Senden".

   Die Aufgabe wird gesendet und die Delegierung gespeichert.

Hinweis: Benutzer, die bereits Stellvertreter sind, erscheinen beim Hinzufügen eines Stellvertreters nicht in den Suchergebnissen.

Weitere Informationen:

Aktivieren der Delegierung (siehe Seite 375)

So entfernen Sie eine Delegierung:

Wenn sich ein Benutzer bei CA IdentityMinder anmeldet, und es bestehen Delegierungen, zeigt CA IdentityMinder folgende Erinnerung an:

```
Sie haben Delegierungen eingerichtet. Prüfen Sie, ob sie weiterhin erforderlich sind.
```

So entfernen Sie eine Delegierung für Sie selbst:

1. Wählen Sie in der Benutzerkonsole "Startseite", "Abwesenheits-Assistent" aus.

   Das Fenster "Abwesenheits-Assistent" wird geöffnet.

2. Klicken Sie für die Stellvertreter, die Sie entfernen möchten, auf das Minuszeichen (-).

   Die Stellvertreter werden aus der Liste entfernt.

3. Klicken Sie auf "Senden".

   Die Aufgabe wird übermittelt und die Delegierung entfernt.

So entfernen Sie eine Delegierung für einen anderen Benutzer:

1. Wählen Sie in der Benutzerkonsole "Benutzer", "Arbeitselemente verwalten", "Arbeitselemente delegieren" aus.

   Ein Fenster für die Suche nach dem Benutzer wird geöffnet.

2. Suchen Sie nach dem Benutzer, dessen Delegierungen Sie entfernen möchten, und wählen Sie ihn aus.

   Die Liste der Stellvertreter wird angezeigt.

3. Klicken Sie für die Stellvertreter, die Sie entfernen möchten, auf das Minuszeichen (-).

   Die Stellvertreter werden aus der Liste entfernt.

4. Klicken Sie auf "Senden".

   Die Aufgabe wird übermittelt und die Delegierung entfernt.

Hinweis: Sie können einen Stellvertreter nur entfernen, wenn der Benutzer in dem von Ihnen verwalteten Bereich liegt.

Neuzuweisen von Arbeitselementen

Das Neuzuweisen ermöglicht Benutzern und Administratoren, nach Erstellen eines Arbeitselements den zugewiesenen Benutzer zu ändern. Ein Administrator kann folgende Aufgaben durchführen:

- Anzeigen der Arbeitsliste eines anderen Benutzers
- Hinzufügen und Entfernen von zu Arbeitselementen zugewiesenen Benutzern
- Ändern des Reservierungsstatus von Arbeitselementen

Zum Beispiel kann ein Administrator ein Arbeitselement neuzuweisen oder ein für einen Benutzer reserviertes Arbeitselement freigeben, wenn der Benutzer es nicht verwendet.

Wenn ein Arbeitselement für einen Benutzer reserviert ist, während es neu zugewiesen wird, bleibt es für den Benutzer reserviert. Wenn der Benutzer dieses Arbeitselement jedoch freigibt, kann er nicht mehr darauf zugreifen.

Wenn ein Arbeitselement für einen Delegierten reserviert ist, während die Delegierung zurückgezogen wird, hat der Delegierte Zugriff, bis das Arbeitselement abgeschlossen ist oder freigegeben wird.

Weitere Informationen:

Neue Zuweisung und reservierte Arbeitselemente (siehe Seite 373)

Die Registerkarte "Genehmiger"

Sie führen die Neuzuordnung auf der Registerkarte "Genehmiger" für Arbeitselemente aus, die eine Liste von aktuellen Arbeitselementsgenehmigern (oder zugewiesenen Benutzern) anzeigt. Wenn Sie eine Neuzuordnung ausführen, weisen Sie das offene Arbeitselement allen Genehmigern in der Liste zu. Daher müssen Sie, um ein Arbeitselement einem anderen Benutzer zuzuweisen, auch den aktuellen zugewiesenen Benutzer entfernen.

Neuzuweisen von Arbeitselementen

Die Neuzuweisung eines Arbeitselements von einem Benutzer zu einem anderen umfasst zwei Schritte:

- Ein neuer Genehmiger wird ausgewählt.
- Der aktuelle Genehmiger wird entfernt.

Hinweis: Die Benutzer, für die Sie das Arbeitselement neu zuweisen möchten, müssen in Ihrem Bereich liegen.

So weisen Sie Ihr eigenes Arbeitselement neu zu

1. Wählen Sie "Startseite", "Meine Arbeitsliste anzeigen".

   Ihre Arbeitsliste wird angezeigt.

2. Wählen Sie ein Arbeitselement aus, um es zu erweitern.

3. Wählen Sie die Registerkarte "Genehmiger" aus.

   Eine Liste mit allen aktuellen Genehmigern, einschließlich des Benutzers, dessen Arbeitsliste Sie verwalten, wird angezeigt.

4. Klicken Sie auf Zugewiesene Benutzer hinzufügen.

   Ein Fenster für die Auswahl des Benutzers wird geöffnet.

5. In diesem Fenster können Sie die Benutzer suchen, denen Sie Arbeitselemente neu zuweisen möchten.

   Hinweis: Für die Genehmigungsmodi ALL und SUBSET können Sie ein Arbeitselement nur *einem* Benutzer neu zuweisen.

6. Klicken Sie auf die Schaltfläche mit dem Minuszeichen (-), um sich als zugewiesenen Benutzer zu entfernen.

7. Klicken Sie auf "Neuzuordnung ausführen".

   Das Arbeitselement wird in den Arbeitslisten der neu zugewiesenen Benutzer angezeigt.

Hinweis: Ein Administrator kann das Arbeitselement eines anderen Benutzers neu zuweisen, reservieren oder freigeben, aber er kann es nicht genehmigen oder ablehnen. Diese Aufgaben kann nur der Besitzer des Arbeitselements durchführen.

So weisen Sie das Arbeitselement eines anderen Benutzers neu zu

1. Wählen Sie "Benutzer", "Arbeitselemente verwalten", "Arbeitselemente des Benutzers verwalten".

   Ein Fenster für die Auswahl des Benutzers wird geöffnet.

2. Suchen Sie den Benutzer, dessen Arbeitselemente Sie neu zuweisen möchten, und klicken Sie auf "Auswählen".

   Das Fenster "Arbeitselemente des Benutzers verwalten" wird angezeigt.

3. Wählen Sie ein Arbeitselement aus, um es zu erweitern.

4. Wählen Sie die Registerkarte "Genehmiger" aus.

   Eine Liste mit allen aktuellen Genehmigern, einschließlich des Benutzers, dessen Arbeitsliste Sie verwalten, wird angezeigt.

5. Klicken Sie auf Zugewiesene Benutzer hinzufügen.

   Ein Fenster für die Auswahl des Benutzers wird geöffnet.

6. In diesem Fenster können Sie die Benutzer suchen, denen Sie Arbeitselemente neu zuweisen möchten.

7. Klicken Sie auf die Schaltfläche mit dem Minuszeichen (-), um den aktuell zugewiesenen Benutzer zu entfernen.

8. Klicken Sie auf "Neuzuordnung ausführen".

   Das Arbeitselement wird in den Arbeitslisten der neu zugewiesenen Benutzer angezeigt.

Massenvorgänge für Arbeitselemente

Ab dieser Version von CA IdentityMinder können die folgenden Massenvorgänge auf ausgewählten Arbeitselementen ausgeführt werden:

- Genehmigen
- Ablehnen
- Reservieren
- Freigeben

In der Benutzerkonsole wurde die Registerkarte zum Konfigurieren der Arbeitsliste um das neue Kontrollkästchen "Unterstützt Massenvorgänge" erweitert. Wenn dieses Kontrollkästchen aktiviert ist, kann der Benutzer Massengenehmigungen, -ablehnungen, -freigaben und -reservierungen von Arbeitselementen durchführen, deren Eigentümer er ist oder die an ihn delegiert wurden. Administratoren können diese Massenvorgänge auf Arbeitselementen nur mithilfe der Aufgabe "Arbeitselemente des Benutzers verwalten" ausführen.

Hinweis: Massenvorgänge können für keine Aufgaben des Typs "Anzeigen" wie "Meine Arbeitsliste anzeigen" aktiviert werden.

Konfigurieren der Registerkarte "Arbeitsliste" für Massenvorgänge

Gehen Sie wie folgt vor, um die Registerkarte "Arbeitsliste" für die Unterstützung von Massenvorgängen auf der Aufgabenebene zu konfigurieren.

Auf der Registerkarte "Rollen und Aufgaben" in der Benutzerkonsole

1. Wählen Sie "Manage Tasks" (Aufgaben verwalten), "Admin-Aufgabe ändern", und klicken Sie auf "Suchen".
2. Wählen Sie "Arbeitselemente in Benutzer verwalten".
3. Klicken Sie auf der Registerkarte "Registerkarten" auf das Stift-Symbol neben "Arbeitsliste".

   Das Fenster "Configure Work List" (Arbeitsliste konfigurieren) wird angezeigt.
4. Wählen Sie "Unterstützt Massenvorgänge".

   Jetzt sind Massenvorgänge auf der Aufgabenebene verfügbar.

Kapitel 13: E-Mail-Benachrichtigungen

Dieses Kapitel enthält folgende Themen:

E-Mail-Benachrichtigungen in CA IdentityMinder (siehe Seite 386)
Auswählen einer E-Mail-Benachrichtigungsmethode (siehe Seite 387)
Konfigurieren vom SMTP-Einstellungen (siehe Seite 388)
Erstellen von E-Mail-Benachrichtigungsrichtlinien (siehe Seite 391)
Verwenden von E-Mail-Vorlagen (siehe Seite 401)

E-Mail-Benachrichtigungen in CA IdentityMinder

E-Mail-Benachrichtigungen informieren die Benutzer von CA IdentityMinder über Aufgaben und Ereignisse im System. Beispielsweise kann CA IdentityMinder eine E-Mail an Genehmiger senden, wenn ein Ereignis oder eine Aufgabe eine Genehmigung erfordert.

CA IdentityMinder bietet die folgenden Methoden zum Konfigurieren von E-Mail-Benachrichtigungen:

- **E-Mail-Benachrichtigungsrichtlinien**

  E-Mail-Benachrichtigungsrichtlinien ermöglichen Geschäftsadministratoren das Erstellen, Anzeigen, Ändern und Löschen von E-Mail-Benachrichtigungen mit Hilfe von Aufgaben in der Benutzerkonsole. Zum Erstellen von E-Mail-Benachrichtigungen ist keine Kodierung erforderlich.

  Administratoren können den Inhalt einer E-Mail, ihren Sendezeitpunkt und ihren Empfänger definieren. Der Inhalt der E-Mail, der in einem HTML-Editor definiert wird, kann dynamische Informationen wie aktuelle Datums- oder Ereignisinformationen enthalten, die CA IdentityMinder nach dem Versenden der E-Mail einfügt. Beispielsweise können Sie eine E-Mail-Benachrichtigung konfigurieren, die an einen Genehmiger gesendet wird, wenn ein neuer Benutzer erstellt wird. Die E-Mail kann die Anmeldeinformationen, das Einstellungsdatum und den Manager des Benutzers enthalten.

  Hinweis: Richtlinien für E-Mail-Benachrichtigungen sind Policy Xpress-Richtlinien, (siehe Seite 511) die von einem getrennten Aufgabensatz erstellt und verwaltet werden.

- **E-Mail-Vorlagen**

  Bei dieser Methode werden E-Mail-Benachrichtigungen aus E-Mail-Vorlagen generiert. CA IdentityMinder bietet standardmäßige E-Mail-Vorlagen, die so verwendet werden können, wie sie installiert wurden, oder von Systemadministratoren angepasst werden können. Diese Administratoren verwenden eine E-Mail-Vorlagen-API zur Angabe von dynamischen Inhalten, wie z. B. der Empfängerliste, und Informationen zu dem Ereignis, das die E-Mail auslöst.

CA IdentityMinder kann E-Mail-Benachrichtigungen generieren, wenn Folgendes auftritt:

- Ein Ereignis, das von einem Workflow-Genehmiger genehmigt oder abgelehnt werden muss, ist ausstehend

  Hinweis: Bei einem Workpoint-Genehmigungsprozess mit mehreren Genehmigungsaktivitäten sendet die in den Benutzerkonsolenaufgaben konfigurierte E-Mail-Benachrichtigung eine Benachrichtigung für jede Aktivität. Wenn Sie die E-Mail-Vorlagen für dieselbe Benachrichtigung verwenden, wird nur eine E-Mail an die Genehmiger gesendet (wenn das Ereignis den Status "Ausstehend" erreicht).

- Ein Genehmiger genehmigt ein Ereignis oder eine Aufgabe

- Ein Genehmiger lehnt ein Ereignis oder eine Aufgabe ab
- Ein Ereignis oder eine Aufgabe startet, schlägt fehl oder wird abgeschlossen
- Ein Benutzer wird erstellt oder geändert

Konfigurieren Sie Ihre SMTP-Einstellungen (siehe Seite 388), um CA IdentityMinder-E-Mail-Benachrichtigungen zu verwenden. Wenn Sie die E-Mail-Vorlagenmethode verwenden, aktivieren Sie in CA IdentityMinder auch E-Mail-Benachrichtigungen.

Auswählen einer E-Mail-Benachrichtigungsmethode

In der folgenden Tabelle werden die Unterschiede zwischen den Richtlinien für E-Mail-Benachrichtigungen und den E-Mail-Vorlagen zusammengefasst:

Aktivität	E-Mail-Verwaltungsaufgaben	E-Mail-Vorlagen
Konfigurieren von E-Mail-Benachrichtigungen	Administratoren verwenden Admin-Aufgaben in der Benutzerkonsole, um E-Mail-Benachrichtigungen zu erstellen, zu ändern, anzuzeigen und zu löschen.	Administratoren ändern Standardvorlagen in den CA IdentityMinder-Verwaltungstools.
Konfigurieren des Zeitpunkts für das Senden von E-Mails	CA IdentityMinder kann E-Mail-Benachrichtigungen generieren, wenn bestimmte Ereignisse oder Aufgaben auftreten. Die E-Mail-Verwaltungsaufgaben und die E-Mail-Vorlagen unterstützen die gleichen Ereignisse und Aufgaben. Die E-Mail-Verwaltungsaufgaben bieten in einigen Fällen jedoch mehr Granularität. E-Mail-Benachrichtigungen werden für die folgenden Aufgaben und Ereignisse unterstützt: ■ Ein Ereignis, das von einem Workflow-Genehmiger genehmigt oder abgelehnt werden muss, ist ausstehend ■ **Hinweis:** Bei einem Workpoint-Genehmigungsprozess mit mehreren Genehmigungsaktivitäten sendet die mit den E-Mail-Verwaltungsaufgaben konfigurierte E-Mail-Benachrichtigung eine Benachrichtigung für jede Aktivität. Wenn Sie die E-Mail-Vorlagen für dieselbe Benachrichtigung verwenden, wird nur eine E-Mail an die Genehmiger gesendet (wenn das Ereignis den Status "Ausstehend" erreicht). ■ Ein Genehmiger genehmigt ein Ereignis oder eine Aufgabe ■ Ein Genehmiger lehnt ein Ereignis oder eine Aufgabe ab ■ Ein Ereignis oder eine Aufgabe startet, schlägt fehl oder wird abgeschlossen ■ Ein Benutzer wird erstellt oder geändert	

Aktivität	E-Mail-Verwaltungsaufgaben	E-Mail-Vorlagen
Hinzufügen von dynamischem Inhalt zu E-Mails	Administratoren können auf der Registerkarte "Inhalt" der Aufgaben "Create Email" (E-Mail erstellen) oder "Modify Email" (E-Mail ändern) über die Auswahl aus einer Liste mit Optionen dynamischen Inhalt im Text einer E-Mail-Nachricht hinzufügen. CA IdentityMinder fügt den dynamischen Inhalt basierend auf Informationen im Ereignis oder in der Aufgabe, das bzw. die die Benachrichtigung auslöst, automatisch ein.	Administratoren verwenden die E-Mail-Vorlagen-API, um die E-Mail-Standardvorlagen anzupassen, die verwendet werden, um E-Mail-Benachrichtigungen zu generieren.
Unterstützen von vorhandenen E-Mail-Benachrichtigungen	E-Mail-Benachrichtigungen, die mithilfe der E-Mail-Verwaltungsaufgaben konfiguriert werden, basieren auf Policy Xpress-Richtlinien. Wenn Sie ein Upgrade von CA IdentityMinder Option Pack 1 auf CA IdentityMinder 12.6.3 durchgeführt haben, können die in Policy Xpress konfigurierten E-Mail-Benachrichtigungen weiterhin verwendet werden. Diese E-Mail-Benachrichtigungen werden jedoch anstelle von Policy Xpress mithilfe der E-Mail-Verwaltungsaufgaben verwaltet.	E-Mail-Benachrichtigungen, die Sie mithilfe der E-Mail-Vorlagenmethode in einer Vorgängerversion von CA IdentityMinder erstellt haben, können in CA IdentityMinder 12.6.3 weiterhin verwendet werden.

Konfigurieren vom SMTP-Einstellungen

Konfigurieren Sie die SMTP-Einstellungen, bevor Sie E-Mail-Benachrichtigungen aktivieren. Hinweise zum Konfigurieren der SMTP-Einstellungen für Ihren Anwendungsserver finden Sie in den folgenden Abschnitten.

Konfigurieren von SMTP-Einstellungen auf JBoss

1. Öffnen Sie den Mail-Dienstbereitstellungs-Deskriptor in einem Texteditor wie folgt:

   Einzelner Knoten: *jboss_home*\server\default\deploy\mail-service.xml

   Cluster: *jboss_home*\server\all\deploy\mail-service.xml

2. Ändern Sie die mail.smtp.host-Eigenschaft mit dem Namen Ihres SMTP-Servers folgendermaßen:

   ```
   <-- Change to the SMTP gateway server -->
   <property name="mail.smtp.host" value="your_smtp_server "/>
   ```

   Beispiel:

   ```
   <property name="mail.smtp.host" value="smtp.mailserver.company.com"/>
   ```

3. Speichern Sie die Datei "mail-service.xml".

4. Öffnen Sie die folgende E-Mail-Eigenschaftsdatei in einem Texteditor:

   Einzelner Knoten:
   jboss_home\server\default\deploy\iam_im.ear\config\com\netegrity\config\email.properties

   Cluster:*jboss_home*\server\all\farm\iam_im.ear\config\com\netegrity\config\email.properties

5. Um die Absenderadresse für E-Mails einzurichten, die von einem Workflow generiert werden, suchen Sie nach der admin.email.address-Eigenschaft, und legen Sie den Wert auf die entsprechende E-Mail-Adresse fest. Beispiel:

   ```
   admin.email.address=admin@company.com
   ```

6. Wenn Sie die E-Mail-Vorlagenmethode verwenden, aktivieren Sie E-Mail-Benachrichtigungen in der Management-Konsole.

   E-Mail-Benachrichtigungen müssen in der Management-Konsole nicht aktiviert werden, wenn Sie Richtlinien für E-Mail-Benachrichtigungen verwenden.

Konfigurieren von SMTP-Einstellungen auf WebLogic

Sie konfigurieren E-Mail-Einstellungen in der WebLogic-Server-Verwaltungskonsole und in einer email.properties-Datei.

So konfigurieren Sie E-Mail-Einstellungen für WebLogic

1. Erstellen Sie in der WebLogic-Server-Verwaltungskonsole eine Mailsitzung mit den folgenden Eigenschaften:
   - **mail.smtp.host**-Eigenschaft: Legen Sie diesen Wert auf Ihren SMTP-Server fest. Zum Beispiel: mail.smtp.host=mymailserver.company.com
   - **mail.transport.protocol**-Eigenschaft: Legen Sie diesen Wert auf SMTP fest. Zum Beispiel: mail.transport.protocol=smtp
   - **JNDI-Name**: nete/Mail
   - **Ziel**: WebLogic-Servername
2. Öffnen Sie die folgende E-Mail-Eigenschaftsdatei für CA IdentityMinder in einem Texteditor:

   weblogic_domain\applications\iam.ear\config\com\netegrity\config\email.properties
3. Richten Sie die Absenderadresse für E-Mails, die von einem Workflow generiert werden, ein, indem Sie nach der admin.email.address-Eigenschaft suchen und den Wert auf die entsprechende E-Mail-Adresse festlegen. Beispiel:
   `admin.email.address=admin@company.com`
4. Aktivieren Sie die E-Mail-Benachrichtigung in der Management-Konsole.

   Hinweis: E-Mail-Benachrichtigungen müssen in der Management-Konsole nicht aktiviert werden, wenn Sie Richtlinien für E-Mail-Benachrichtigungen verwenden.

Konfigurieren von SMTP-Einstellungen auf WebSphere

Das imsSetup-Hilfsprogramm, das Sie nach dem Installieren der CA IdentityMinder-Komponenten ausführen, konfiguriert ein neues Mailsitzungsobjekt mit der Bezeichnung "mailMail".

Damit die E-Mail-Benachrichtigungsfunktion ordnungsgemäß ausgeführt wird, geben Sie im Feld "Mail Transport Host" für die mailMail-Sitzung den Server an, mit dem WebSphere eine Verbindung herstellt, wenn E-Mails gesendet werden.

Die mailMail-Sitzung befindet sich in der WebSphere-Verwaltungskonsole unter "Ressourcen", "Mail Providers" (Mail-Anbieter), "Built-in Mail Provider" (Integrierter Mail-Anbieter), "Mail Sessions" (Mail-Sitzungen), "mailMail".

Hinweis: Um das mailMail-Objekt anzuzeigen, ändern Sie den Geltungsbereich im Fenster "Mail Session" (Mail-Sitzungen) in Server. Wenn Sie den Geltungsbereich nicht in Server ändern, wird das mailMail-Objekt nicht angezeigt.

Weitere Informationen zum Konfigurieren eines WebSphere-Mail-Anbieters finden Sie in der WebSphere-Dokumentation.

Wenn Sie die E-Mail-Vorlagenmethode verwenden, aktivieren Sie die E-Mail-Benachrichtigung in der Management-Konsole, nachdem Sie die SMTP-Einstellungen konfiguriert haben.

Hinweis: E-Mail-Benachrichtigungen müssen in der Management-Konsole nicht aktiviert werden, wenn Sie Richtlinien für E-Mail-Benachrichtigungen verwenden.

Erstellen von E-Mail-Benachrichtigungsrichtlinien

Sie können die Benutzerkonsole zum Erstellen von E-Mail-Benachrichtigungsrichtlinien verwenden, die E-Mails versenden, wenn bestimmte Aktionen durchgeführt werden. Beispielsweise können Sie eine E-Mail-Benachrichtigungsrichtlinie erstellen, die eine E-Mail versendet, um Genehmiger über die Erstellung eines neuen Benutzers zu informieren.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "System" die Option "E-Mail" und anschließend "E-Mail erstellen".
2. Wählen Sie eine der folgenden Optionen aus:
   - Neues Objekt des Typs "Verwaltete E-Mail" erstellen
   - Kopie eines Objekts des Typs "Verwaltete E-Mail" erstellen

     Verwendet eine vorhandene E-Mail-Benachrichtigungsrichtlinie als Vorlage für die Erstellung einer neuen Richtlinie.
3. Geben Sie auf der Registerkarte "Profil" grundlegende Informationen zu der E-Mail-Benachrichtigungsrichtlinie an.

4. Legen Sie auf der Registerkarte "Sendezeitpunkt" fest, wann CA IdentityMinder die E-Mail versenden soll.

   Die Registerkarte "Sendezeitpunkt" bietet verschiedene Optionen, um anzugeben, welche Aktionen E-Mail-Benachrichtigungen auslösen sollen.

5. Geben Sie auf der Registerkarte "Empfänger" die Empfänger der E-Mail an.

6. Definieren Sie auf der Registerkarte "Inhalt" den Betreff und den Inhalt der E-Mail.

   Sie können im E-Mail-Inhalt dynamische Inhalte, wie z. B. das Datum, die Aufgabe oder den Ereignisnamen, und Benutzerattribute angeben.

Weitere Informationen:

Registerkarte "Sendezeitpunkt" (siehe Seite 393)
Registerkarte "Empfänger" (siehe Seite 395)
Inhalt (siehe Seite 396)
Registerkarte "Profil" für E-Mail-Benachrichtigungen (siehe Seite 392)

Registerkarte "Profil" für E-Mail-Benachrichtigungen

Auf der Registerkarte "Profil" in den E-Mail-Verwaltungsaufgaben können Sie grundlegende Informationen zu einer E-Mail-Benachrichtigungsrichtlinie angeben. Diese Registerkarte enthält die folgenden Felder:

E-Mail-Name

Gibt die E-Mail-Benachrichtigungsrichtlinie in der Benutzerkonsole an.

Hinweis: Der E-Mail-Name wird nicht angezeigt, wenn die E-Mail gesendet wird. Der Name wird nur zum Verwalten der E-Mail-Benachrichtigungsrichtlinie in der Benutzerkonsole verwendet.

Kategorie

Unterteilt E-Mail-Benachrichtigungsrichtlinien in Gruppen, um die Verwaltung zu vereinfachen.

Geben Sie eine vorhandene Kategorie an, indem Sie sie in der Dropdown-Liste auswählen, oder wählen Sie die Schaltfläche für die zweite Option aus, und geben Sie den Namen einer neuen Kategorie ein.

Beschreibung

Beschreibt die E-Mail-Benachrichtigungsrichtlinie für Administratoren.

Die Beschreibung wird nicht angezeigt, wenn die E-Mail gesendet wird.

Aktiviert

Gibt an, dass CA IdentityMinder die E-Mail sendet, wenn die auf der Registerkarte "Sendezeitpunkt" definierten Bedingungen erfüllt sind.

Benutzerdefinierte Daten

Erstellt in Policy Xpress ein benutzerdefiniertes Datenelement, das zum Konfigurieren von benutzerdefinierten Empfängern oder Inhalten verwendet werden kann.

Benutzerdefinierte Datenelemente können auch in anderen Datenelementen als Parameter verwendet werden.

Hinweis: Der Abschnitt Daten (siehe Seite 518) enthält weitere Informationen zu Datenelementen.

Wenn Sie auf "Benutzerdefinierte Daten" klicken, öffnet CA IdentityMinder ein Fenster, in dem Sie neue Datenelemente hinzufügen können.

Eintrittsregeln

Definiert Regeln für den Versand von E-Mail-Benachrichtigungen durch CA IdentityMinder in Fällen, in denen die Standardregeln auf der Registerkarte "Sendezeitpunkt" nicht differenziert genug sind.

Beispielsweise bietet die Registerkarte "Sendezeitpunkt" eine Standardregel, die E-Mails sendet, wenn ein Attribut eines Benutzerprofils geändert wird. Wenn Sie möchten, dass CA IdentityMinder nur dann eine E-Mail sendet, wenn sich die Abteilung eines Benutzers ändert, können Sie eine benutzerdefinierte Eintrittsregel erstellen. (In diesem Fall erstellen Sie ein benutzerdefiniertes Datenelement, das die Änderung der Abteilung identifiziert, und anschließend eine Eintrittsregel, die das von Ihnen erstellte benutzerdefinierte Datenelement verwendet.)

Hinweis: Weitere Informationen hierzu finden Sie im Abschnitt Eintrittsregeln (siehe Seite 521).

Registerkarte "Sendezeitpunkt"

CA IdentityMinder bietet verschiedene Standardoptionen, die bestimmen, wann eine E-Mail versendet wird. Einige dieser Optionen erfordern zusätzliche Informationen, z. B. einen Aufgaben- oder Ereignisnamen. Beispielsweise erfordert das Senden einer E-Mail beim Start einer Aufgabe die Auswahl der Aufgabe, die die E-Mail auslöst.

Sie können eine oder mehrere der folgenden Optionen auf der Registerkarte "Sendezeitpunkt" auswählen:

Benutzer erstellt

Sendet eine E-Mail, wenn ein Benutzer erstellt wurde. Die E-Mail wird nach der Fertigstellung des Ereignisses "CreateUserEvent" gesendet.

Benutzer geändert

Sendet eine E-Mail, wenn ein Benutzer geändert wurde. Die E-Mail wird nach der Fertigstellung des Ereignisses "ModifyUserEvent" gesendet.

Workflow ausstehend

Eine E-Mail wird gesendet, wenn ein Workflow-Prozess einen Genehmiger zuweist. Wenn Sie diese Option auswählen, geben Sie den entsprechenden Workflow-Prozess an. Eine E-Mail, die mit dieser Richtlinie definiert ist, sendet bei jedem Schritt des ausgewählten Workflow-Vorgangs eine individuelle E-Mail an Genehmiger.

Ausstehende Workflow-E-Mail

Eine E-Mail wird gesendet, wenn ein Workflow-Vorgang eine angegebene Aktivität erreicht. Wenn Sie diese Option auswählen, geben Sie den entsprechenden Workflow-Prozess an. Eine E-Mail, die mit dieser Richtlinie definiert ist, sendet für jeden Genehmigungsschritt eine individuelle E-Mail-Benachrichtigung.

Ereignis hat begonnen

Sendet eine E-Mail, wenn ein Ereignis den Status "Vor" erreicht. Wenn Sie diese Option auswählen, geben Sie das Ereignis an.

Hinweis: Wenn Sie "Ereignis hat begonnen" festlegen, und die E-Mail nicht versendet wird, wird das zur Benachrichtigung zugeordnete Ereignis nicht ausgeführt.

Ereignis beendet

Sendet eine E-Mail, wenn ein Ereignis den Status "Nach" erreicht. Wenn Sie diese Option auswählen, geben Sie das Ereignis an.

Ereignis genehmigt

Sendet eine E-Mail, wenn ein Ereignis den Status "Genehmigt" erreicht. Wenn Sie diese Option auswählen, geben Sie das Ereignis an.

Ereignis abgelehnt

Sendet eine E-Mail, wenn ein Ereignis den Status "Abgelehnt" erreicht. Wenn Sie diese Option auswählen, geben Sie das Ereignis an.

Ereignis fehlgeschlagen

Sendet eine E-Mail, wenn ein Ereignis fehlschlägt. Wenn Sie diese Option auswählen, geben Sie das Ereignis an.

Aufgabe gesendet

Sendet eine E-Mail, wenn die Verarbeitung der Aufgabe beginnt. Wenn Sie diese Option auswählen, geben Sie die Aufgabe an.

Aufgabe abgeschlossen

Sendet eine E-Mail, wenn die Aufgabe abgeschlossen ist. Wenn Sie diese Option auswählen, geben Sie die Aufgabe an.

Aufgabe fehlgeschlagen

Sendet eine E-Mail, wenn die Aufgabe fehlschlägt. Wenn Sie diese Option auswählen, geben Sie die Aufgabe an.

Registerkarte "Empfänger"

Sie können mehrere Empfänger für die Felder "An", "CC" oder "BCC" einer E-Mail konfigurieren. Die Empfängerliste kann statisch sein oder von dem Aktionstyp, der die E-Mail auslöst, sowie von den beteiligten Benutzern abhängen.

Wählen Sie zur Angabe von Empfängern das Symbol "Bearbeiten" neben dem Feld "An", "CC" oder "BCC" auf der Registerkarte "Empfänger" aus. Wählen Sie anschließend eine der folgenden Optionen aus, mit denen Sie die Liste der Empfänger konfigurieren können:

Workflow-Genehmiger

Sendet die E-Mail an alle Genehmiger im Workflow-Prozess. Diese Option ist nur verfügbar, wenn die E-Mail für ein "Workflow ausstehend"-Ereignis gesendet wird.

Manager

Sendet die E-Mail an den Manager des Benutzers, für den die Aufgabe ausgeführt wurde.

Hinweis: Konfigurieren Sie für die Verwendung der Empfängeroption "Manager" das Managerattribut für die Umgebung. Gehen Sie zum Konfigurieren des Managerattributs in der Managementkonsole zu "Umgebungen", *EnvironmentName*, "Erweiterte Einstellungen", "Sonstige". Legen Sie für "managerattribute" den Namen des physischen Attributs fest, in dem der eindeutige Name des Managers eines Benutzers gespeichert ist.

Geben Sie für relationale Datenbanken das Attribut im folgenden Format an:

Tabellenname.Attribut

Gruppenmitglieder

Sendet die E-Mail an alle Mitglieder einer Gruppe. Wenn Sie diese Option auswählen, wird eine Dropdown-Liste mit verfügbaren Gruppennamen geöffnet.

Rollenmitglieder

Sendet die E-Mail an alle Mitglieder einer Admin-Rolle. Wenn Sie diese Option auswählen, wird eine Dropdown-Liste mit verfügbaren Rollennamen geöffnet.

Statische Adresse

Sendet die E-Mail an eine ausgewählte E-Mail-Adresse. Sie können die E-Mail-Adresse in dem verfügbaren zusätzlichen Textbereich angeben.

Hinweis: Geben Sie im Textbereich nicht mehr als eine Adresse an.

Benutzer

Sendet die E-Mail an den Benutzer, für den die Aufgabe ausgeführt wurde.

Initiator der Aufgabe

Sendet die E-Mail an die Person, die die Anfrage gestellt hat.

Benutzerdefiniert

Ermöglicht Ihnen, zur Definition der Empfänger ein benutzerdefiniertes Datenelement auszuwählen.

Wenn Sie die Option "Benutzerdefiniert" auswählen, wird eine Dropdown-Liste mit den benutzerdefinierten Datenelementen angezeigt, die zur Verwendung verfügbar sind.

Hinweis: Der Abschnitt Daten (siehe Seite 518) enthält weitere Informationen zu Datenelementen.

Inhalt

Sie können den Betreff und den Text einer E-Mail mit einfachem Text definieren oder sie mit dynamischen Inhalten hinzufügen, die beim Senden der E-Mail berechnet werden.

Die Betreffzeile ist ein Feld für reinen Text, in das Sie den gewünschten Text eingeben können. Dieser Text ist der Betreff der E-Mail.

Der Haupttext der E-Mail wird in einem HTML-Editor angezeigt. Sie können beliebigen Text als Haupttext der E-Mail einfügen und formatieren.

Um dynamische Inhalte einzubeziehen, wählen Sie Optionen in einer Dropdown-Liste aus. Der Editor fügt an der Position des Mauszeigers Indikatoren für dynamische Inhalte ein, die folgendermaßen aussehen:

{*Typ*}

Typ steht für einen der unterstützten dynamischen Inhaltstypen.

Wenn Sie beispielsweise den dynamischen Inhaltstyp "Attribute" auswählen und das Attribut "FirstName" angeben, zeigt der HTML-Editor auf der Registerkarte "Inhalt" Folgendes an:

{'Attribute: FirstName'}

Hinweis: Verwenden Sie zum Hinzufügen dynamischer Inhalte zur Betreffzeile die Dropdown-Liste unter der Betreffzeile. Um dynamische Inhalte im Haupttext der E-Mail hinzuzufügen, verwenden Sie die Dropdown-Liste unter dem Inhaltsfeld.

Wenn die E-Mail-Nachricht gesendet wird, ersetzt CA IdentityMinder die dynamischen Inhalte durch den entsprechenden Text. Die im HTML-Editor festgelegte Formatierung des Textes, z. B. Fettdruck, wird beibehalten.

Zu den dynamischen Inhaltstypen gehören:

Datum

Gibt das aktuelle Datum im von Ihnen festgelegten Format an.

Aufgabe

Gibt die Aufgabe an, für die die E-Mail gesendet wird.

Objektname

Gibt den Namen des Objekts in dem Ereignis an, das die E-Mail auslöst. Wenn das Ereignis ein Benutzerereignis ist, enthält dieses Feld den Anmeldenamen des Benutzers.

Bei dem Objekt muss es sich nicht um einen Benutzer handeln. Beispielsweise kann das Objekt ein beliebiges verwaltetes Objekt sein, wie eine Gruppe, eine Admin-Rolle usw.

Attribut

Gibt den Wert eines der Benutzerattribute an. Der Benutzer ist das Subjekt der Aufgabe. Diese Option erfordert die Auswahl des Attributs aus einer Dropdown-Liste.

Managerattribut

Gibt den Wert eines der Attribute des Managers des Benutzers an. Der Benutzer ist das Subjekt der Aufgabe. Diese Option erfordert die Auswahl des Attributs aus einer Dropdown-Liste.

Hinweis: Konfigurieren Sie für die Verwendung der Empfängeroption "Manager" das Managerattribut für die Umgebung. Gehen Sie zum Konfigurieren des Managerattributs in der Managementkonsole zu "Umgebungen", *EnvironmentName*, "Erweiterte Einstellungen", "Sonstige". Legen Sie für "managerattribute" den Namen des physischen Attributs fest, in dem der eindeutige Name des Managers eines Benutzers gespeichert ist.

Geben Sie für relationale Datenbanken das Attribut im folgenden Format an:

Tabellenname.Attribut

Benutzerdefiniert

Ermöglicht Ihnen, zur Definition der Empfänger ein benutzerdefiniertes Datenelement auszuwählen.

Wenn Sie die Option "Benutzerdefiniert" auswählen, wird eine Dropdown-Liste mit den benutzerdefinierten Datenelementen angezeigt, die zur Verwendung verfügbar sind.

Hinweis: Der Abschnitt Daten (siehe Seite 518) enthält weitere Informationen zu Datenelementen.

Ändern von E-Mail-Benachrichtigungsrichtlinien

Sie ändern eine vorhandene E-Mail-Benachrichtigungsrichtlinie, um sie an Ihre Geschäftsanforderungen anzupassen.

So ändern Sie eine E-Mail-Benachrichtigungsrichtlinie:

1. Wählen Sie "System", "E-Mail" und anschließend "E-Mail ändern".

   CA IdentityMinder zeigt ein Suchfenster an.

2. Wählen Sie die zu ändernde E-Mail-Benachrichtigungsrichtlinie aus.
3. Ändern Sie bei Bedarf die Einstellungen auf den Registerkarten "Profil", "Sendezeitpunkt", "Empfänger" und "Inhalt".

Deaktivieren von E-Mail-Benachrichtigungsrichtlinien

Sie können E-Mail-Benachrichtigungsrichtlinien über das Kontrollkästchen "Aktiviert" auf der Registerkarte "Profil" aktivieren oder deaktivieren, wenn Sie eine E-Mail-Benachrichtigungsrichtlinie erstellen oder ändern. Wenn eine E-Mail-Benachrichtigungsrichtlinie deaktiviert ist, ist die ausgewählte E-Mail nicht aktiv, und es wird keine E-Mail gesendet.

Hinweis: E-Mail-Benachrichtigungsrichtlinien sind standardmäßig aktiviert.

Anwendungsfall: Senden einer Begrüßungs-E-Mail

Wenn ein neuer Mitarbeiter eingestellt wird, möchte Forward, Inc. eine E-Mail an diesen Benutzer senden, um ihn in der Firma willkommen zu heißen. Die E-Mail muss dem neuen Mitarbeiter wichtige Informationen bieten, z. B. Links zur Mitarbeiter-Homepage und Informationen zu seinem Manager und seiner Abteilung.

Zum Erstellen der E-Mail verwendet der Administrator der Personalabteilung die Aufgabe "E-Mail erstellen" in der Benutzerkonsole, um die folgenden Einstellungen zu konfigurieren:

- Wählen Sie auf der Registerkarte "Sendezeitpunkt" die Option "Benutzer erstellt" aus.
- Führen Sie auf der Registerkarte "Empfänger" die folgenden Schritte aus:
  - Klicken Sie auf das Symbol "Bearbeiten" neben dem Feld "An".

    Wählen Sie "Benutzer", und klicken Sie anschließend auf das Pluszeichen. Wählen Sie den Manager nach derselben Methode aus, und klicken Sie anschließend auf "OK".
  - Klicken Sie auf das Symbol "Bearbeiten" neben dem Feld "CC".

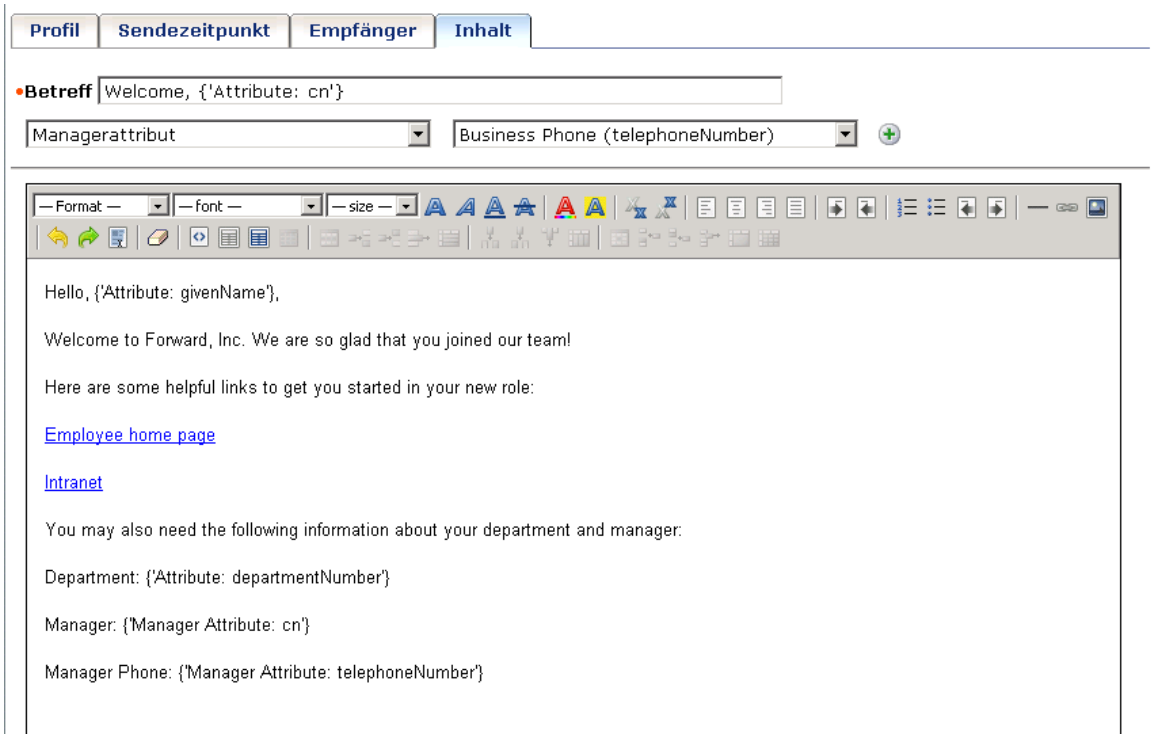
    Wählen Sie "Initiator", klicken Sie auf das Pluszeichen, und klicken Sie anschließend auf "OK", um eine Kopie der E-Mail an den Benutzer zu senden, der den Mitarbeiter in CA IdentityMinder erstellt hat.
- Führen Sie auf der Registerkarte "Inhalt" die folgenden Schritte aus:
  - Geben Sie im Feld "Betreff" den folgenden Text ein: Willkommen,

    Wählen Sie in der Dropdown-Liste "Attribut" aus, während der Mauszeiger sich am Ende des eingegebenen Texts befindet. Wählen Sie anschließend in der zweiten Dropdown-Liste "Vollständiger Name" aus, und klicken Sie dann auf das Pluszeichen.

    Die Betreffzeile sieht ungefähr so aus:

    Willkommen, {'Attribute: eTFullName'}

    Hinweis: Der Attributname hängt von dem von Ihnen verwendeten Benutzerspeicher und Attribut ab.
  - Fügen Sie im Feld "Inhalt" einen beliebigen Begrüßungstext hinzu. Geben Sie wie folgt Links zum Mitarbeiterportal an, und verwenden Sie die Optionen für dynamische Inhalte unter dem Feld "Inhalt", um die Abteilung und den Manager des Benutzers sowie die Telefonnummer des Managers anzuzeigen:



Verwenden von E-Mail-Vorlagen

CA IdentityMinder enthält E-Mail-Standardvorlagen, die Sie verwenden können, um E-Mail-Nachrichten zu generieren. Sie können die installierten Vorlagen verwenden oder diese Ihren Geschäftsanforderungen gemäß anpassen.

So verwenden Sie E-Mail-Vorlagen

1. Konfigurieren Sie SMTP-Einstellungen, um das Senden von E-Mail-Benachrichtigungen in CA IdentityMinder zu aktivieren.
2. Aktivieren Sie die E-Mail-Benachrichtigung in der Management-Konsole (siehe Seite 402).
3. Konfigurieren Sie ein Ereignis oder eine Aufgabe, um eine E-Mail zu senden. (siehe Seite 402)
4. (Optional) Passen Sie ggf. die Standardvorlagen an (siehe Seite 408).

Aktivieren von E-Mail-Benachrichtigungen

Sie können E-Mail-Benachrichtigungen für eine CA IdentityMinder-Umgebung aktivieren oder deaktivieren. Wenn Sie E-Mail-Benachrichtigungen aktivieren, sendet CA IdentityMinder E-Mail-Benachrichtigungen für die Ereignisse und Aufgaben, die Sie angeben.

Hinweis: Um die Funktion "Kennwort vergessen" zu verwenden, aktivieren Sie die E-Mail-Benachrichtigung.\

Bevor Sie E-Mail-Benachrichtigungen in CA IdentityMinder aktivieren, konfigurieren Sie die SMTP-Einstellungen (siehe Seite 388) für Ihren Anwendungsserver.

So aktivieren Sie E-Mail-Benachrichtigungen

1. Klicken Sie in der Managementkonsole auf "Umgebungen".

   Eine Liste der CA IdentityMinder-Umgebungen wird angezeigt.
2. Klicken Sie auf die gewünschte Identity Manager-Umgebung.
3. Wechseln Sie zu "Erweiterte Einstellungen", "E-Mail".
4. Aktivieren Sie das Kontrollkästchen "Aktiviert".
5. Konfigurieren Sie die Ereignisse und Aufgaben, die E-Mails auslösen (siehe Seite 402).
6. Klicken Sie auf "Speichern".
7. Starten Sie die Instanz des Anwendungsservers neu, auf der CA IdentityMinder installiert ist.

Konfigurieren von Ereignissen oder Aufgaben, bei denen E-Mails gesendet werden

Wenn E-Mail-Benachrichtigungen aktiviert sind, können Sie eine Liste mit Ereignissen und Aufgaben angeben, die E-Mail-Benachrichtigungen auslösen. Sie können zum Beispiel einrichten, dass E-Mails unter den folgenden Umständen gesendet werden:

- An einen Systemadministrator - nach Abschluss einer Aufgabe, bei der das Benutzerkennwort zurückgesetzt wird.
- An den Manager eines neuen Mitarbeiters - nach Abschluss einer Aufgabe, bei der ein Benutzer erstellt wird. Wenn "AddToGroupEvent" (im Rahmen der Aufgabe "Benutzer erstellen" generiert) genehmigt wurde, kann außerdem eine weitere E-Mail an alle Mitglieder einer Gruppe gesendet werden, der der neue Benutzer hinzugefügt wird.

So geben Sie Ereignisse und Aufgaben an, die E-Mail-Benachrichtigungen auslösen

1. Klicken Sie in der Managementkonsole auf "Umgebungen".

   Eine Liste der CA IdentityMinder-Umgebungen wird angezeigt.

2. Klicken Sie auf die gewünschte CA IdentityMinder-Umgebung.

3. Wechseln Sie zu "Erweiterte Einstellungen", "E-Mail".

   Das Fenster "Email Properties" (E-Mail-Eigenschaften) wird geöffnet.

4. Wählen Sie ggf. die folgenden Kontrollkästchen zum Aktivieren aus:

   - Events E-mail Enabled (E-Mail für Ereignisse aktiviert)

     Aktiviert die E-Mail-Benachrichtigung für CA IdentityMinder-Ereignisse

   - Tasks Email Enabled (E-Mail für Aufgaben aktiviert)

     Aktiviert die E-Mail-Benachrichtigung für CA IdentityMinder-Aufgaben

5. Geben Sie den Speicherort der E-Mail-Vorlagen an, die CA IdentityMinder verwendet, um die E-Mail-Nachrichten zu erstellen.

   Die E-Mail-Vorlagen befinden sich in einem Unterverzeichnis im folgenden Speicherort:

   iam_im.ear\custom\emailTemplates

   Hinweis: Wenn Sie eine E-Mail-Vorlagendatei mit einem Dateinamen in einer anderen Sprache erstellen, sollte die Betriebssystemsitzung in einer Sprache ausgeführt werden, die den Zeichensatz unterstützt.

6. Geben Sie die Ereignisse, bei denen E-Mail-Benachrichtigungen gesendet werden, wie folgt an:

   - Um ein Ereignis hinzuzufügen, wählen Sie das Ereignis im Ereignis-Listenfeld aus, und klicken Sie auf "Hinzufügen".

     CA IdentityMinder fügt das ausgewählte Ereignis der Liste mit Ereignissen hinzu, bei denen E-Mail-Benachrichtigungen gesendet werden.

     Hinweis: Wenn Sie ein Ereignis auswählen, das keinem Workflow-Vorgang zugeordnet ist, sendet CA IdentityMinder eine E-Mail-Benachrichtigung, wenn das Ereignis abgeschlossen ist.

   - Um ein Ereignis zu löschen, aktivieren Sie das Kontrollkästchen des Ereignisses, und klicken Sie dann auf "Löschen".

7. Geben Sie die Aufgaben, bei denen E-Mail-Benachrichtigungen gesendet werden, wie folgt an:

   - Um eine Aufgabe hinzuzufügen, suchen Sie nach der Aufgabe, indem Sie eine Bedingung im ersten Feld auswählen und einen Namen der Aufgabe ins zweite Feld eingeben. Klicken Sie auf "Suchen".

     Sie können einen unvollständigen Namen für die Aufgabe eingeben, indem Sie ein Platzhalterzeichen (*) verwenden. Um zum Beispiel nach einer Erstellungsaufgabe zu suchen, geben Sie "*erstellen" ein.

     Wählen Sie eine oder mehrere Aufgaben aus den Suchergebnissen aus. Klicken Sie auf "Hinzufügen".

     Hinweis: E-Mail-Benachrichtigungen auf Aufgabenebene sind nicht für Aufgaben mit dem Aktionstyp "Anzeigen" oder "Selbstansicht" verfügbar. Um den Aktionstyp einer Aufgabe anzuzeigen, wechseln Sie zu "Admin-Aufgabe ändern", wählen Sie eine Aufgabe aus, und aktivieren Sie das Aktionsfeld im Aufgabenprofil.

   - Um eine Aufgabe zu löschen, aktivieren Sie das Kontrollkästchen der Aufgabe, und klicken Sie dann auf "Löschen".

     Wenn eine Aufgabe gelöscht wird, wird sie aus der Aufgaben-Tabelle entfernt. Die Aufgabe wird nicht gelöscht.

8. Wenn Sie die Konfiguration der Aufgaben und Ereignisse, die E-Mail-Benachrichtigungen auslösen, abgeschlossen haben, klicken Sie auf "Speichern".
9. Starten Sie den Anwendungsserver neu, auf dem CA IdentityMinder installiert ist.

E-Mail-Inhalt

E-Mail-Benachrichtigungen umfassen eine generische Vorlage sowie aufgabenspezifische Details, die der E-Mail über die E-Mail-API hinzugefügt werden. Die folgenden Informationen können zum Beispiel in eine E-Mail für die Aufgabe "Benutzer erstellen" eingefügt werden:

- Name des Administrators, der die Aufgabe ausführt
- Name des neuen Benutzers
- E-Mail-Adresse des Benutzers, Abteilungsname und andere Attributdaten
- Organisation, in der der Benutzer erstellt wird
- Workflow-Genehmigungsstatus und -Genehmigungszeit
- Name der Aufgabe und die Namen der Ereignisse in der Aufgabe

E-Mail-Vorlagen

E-Mail-Benachrichtigungen werden aus E-Mail-Vorlagen generiert. Identity Manager stellt E-Mail-Standardvorlagen bereit, die Sie so verwenden können, oder mit denen Sie Ihre eigenen E-Mail-Vorlagen erstellen können.

Jede E-Mail-Vorlage enthält das Folgende:

- **Übermittlungsinformationen** - Liste der E-Mail-Empfänger. Identity Manager generiert die Liste der Empfänger basierend auf den an der Aufgabe beteiligten Benutzern automatisch. Zum Beispiel wird eine Genehmigungs-E-Mail an alle Personen gesendet, die für diese Aufgabe als Genehmiger eingerichtet sind.
- **Betreff** - Text in der Betreffzeile der Nachricht.
- **Inhalt** - Nachrichtentext. Der Text enthält normalerweise sowohl statischen Text als auch Variablen, die Identity-Manager basierend auf der Aufgabe oder dem Ereignis auflöst, die bzw. das die E-Mail auslöst.

Die E-Mail-Standardvorlagen befinden sich in einem emailTemplates-Verzeichnis, in dem die Identity Manager-Verwaltungstools installiert sind. Der Standardinstallationsort für die Verwaltungstools ist:

- Für Windows - C:\Programme\CA\CA Identity Manager\
- Für UNIX - <Basisverzeichnis>/CA/CA Identity Manager

Das Verzeichnis "emailTemplates" enthält vier Ordner. Jeder Ordner ist einem Aufgaben- oder Ereignisstatus zugeordnet:

Verzeichnis	Inhalt
Genehmigt	defaultEvent.tmpl - Informiert die Empfänger, dass ein Ereignis genehmigt worden ist.

Verzeichnis	Inhalt
Abgeschlossen	■ CertificationNonCertifiedActionCompletedNotification.tmpl - Informiert den Manager, dass eine Non-Compliance-Aktion für einen Mitarbeiter gestartet wurde. ■ CertificationNonCertifiedActionPendingNotification.tmpl - Informiert den Manager, dass eine Non-Compliance-Aktion für einen Mitarbeiter gestartet wird. ■ CertificationRequiredFinalNotification.tmpl - Letzte Erinnerung an einen Manager, dass die Aufgabe "Benutzer zertifizieren" für einen Mitarbeiter abgeschlossen werden muss. ■ CertificationRequiredNotification.tmpl - Informiert den Manager, dass ein Zertifizierungsprozess für einen Mitarbeiter gestartet wurde. Der Manager muss für diesen Mitarbeiter die Aufgabe "Benutzer zertifizieren" abschließen. ■ CertificationRequiredReminderNotification.tmpl - Erinnerung an den Manager, dass die Aufgabe "Benutzer zertifizieren" für einen Mitarbeiter abgeschlossen werden muss. ■ Certify Employee.tmpl - Informiert einen Administrator, dass der Zertifizierungsprozess für einen Mitarbeiter abgeschlossen ist. ■ CreateProvisioningUserNotificationEvent.tmpl - Sendet ein temporäres Kennwort an einen Benutzer, wenn das Konto dieses Benutzers im Bereitstellungsverzeichnis erstellt wird. ■ defaultTask.tmpl - Informiert die Empfänger, dass Identity Manager eine Aufgabe abgeschlossen hat. ■ ForgottenPassword.tmpl - Sendet ein temporäres Kennwort an Benutzer, die die Funktion "Kennwort vergessen" verwendet haben. ■ ForgottenUserID.tmpl - Sendet eine Benutzer-ID an Benutzer, die die Funktion "Benutzer-ID vergessen" verwendet haben. ■ Self Registration.tmpl - Informiert einen Benutzer, dass eine Selbstregistrierungsaufgabe erfolgreich abgeschlossen wurde.
Ausstehend	■ defaultEvent.tmpl - Informiert Genehmiger, dass ein Arbeitslistenelement Eingreifen erfordert. ■ ModifyUserEvent.tmpl - Entspricht der Standardvorlage, enthält jedoch Methoden für das Abrufen von Attributen aus dem von Benutzern verwalteten Objekt.
Abgelehnt	defaultEvent.tmpl - Informiert die Empfänger, dass ein Ereignis abgelehnt worden ist.

Verwenden Sie die Identity Manager-Vorlagen, die im Verzeichnis "*<im_admin_tools_dir>*\Identity Manager\emailTemplates" als Grundlage zum Erstellen benutzerdefinierter E-Mail-Vorlagen installiert sind, sowie die Vorlagenverzeichnisstruktur.

Vorlagenverzeichnisse

Jedes der unter E-Mail-Vorlagen (siehe Seite 405) beschriebenen Vorlagenverzeichnisse wird einem bestimmten Aufgaben- oder Ereignisstatus zugeordnet. Wenn zum Beispiel eine E-Mail für ein Ereignis gesendet werden soll, das in einem Workflow-Vorgang abgelehnt wurde, sucht Identity Manager in einem bereitgestellten Verzeichnis mit dem Namen "rejected" nach der zu verwendenden Vorlage. Identity Manager generiert dann die E-Mail aus der entsprechenden E-Mail-Vorlage im Verzeichnis.

E-Mail-Vorlagen in einem Verzeichnis

Jedes bereitgestellte Vorlagenverzeichnis enthält mindestens eine E-Mail-Vorlage. Wenn eine Aufgabe oder ein Ereignis auftritt, für die bzw. das E-Mail aktiviert ist, sucht Identity Manager im entsprechenden Vorlagenverzeichnis nach einem Vorlagennamen, der dem Namen der Aufgabe oder des Ereignisses entspricht. Wenn keine entsprechende Vorlage gefunden wird, verwendet Identity Manager die Standardvorlage im Verzeichnis. Die Namen der Standardvorlagen sind unter E-Mail-Vorlagen (siehe Seite 405) aufgelistet. Zum Beispiel verwendet Identity Manager "defaultEvent.tmpl" im Verzeichnis "Ausstehend", um Genehmiger darüber zu informieren, dass sie ein neues Arbeitslistenelement haben.

Sätze von Vorlagenverzeichnissen

Ein Satz von Vorlagenverzeichnissen enthält die Verzeichnisse "Genehmigt", "Abgeschlossen", "Ausstehend" und "Abgelehnt". Sie können mehrere Sätze von Vorlagenverzeichnissen bereitstellen und festlegen, dass ein Satz für eine bestimmte Identity Manager-Umgebung verwendet werden soll.

Unter Bereitstellung von E-Mail-Vorlagen (siehe Seite 428) finden Sie Informationen zum Bereitstellen von Vorlagenverzeichnis-Sätzen.

Informationen zum Konfigurieren von E-Mail-Vorlagenverzeichnisse, damit Identity Manager en richtigen Satz für eine bestimmte Umgebung verwendet, finden Sie im *CA Identity Manager-Konfigurationshandbuch*.

Erstellen von E-Mail-Vorlagen

So erstellen Sie benutzerdefinierte E-Mail-Nachrichten

1. Öffnen Sie die Vorlage, die Sie ändern möchten.

   Wenn Sie zum Beispiel eine E-Mail-Nachricht für das ausstehende Ereignis "Benutzer erstellen" erstellen möchten, öffnen Sie "defaultEvent.tmpl" im Verzeichnis "Ausstehend".

2. Speichern Sie die Vorlage im gleichen Verzeichnis mit einem neuen Namen. Der Name muss mit dem Namen des Ereignisses übereinstimmen, auf das sich die E-Mail bezieht, und die Erweiterung ".tmpl" haben.

   Nennen Sie die Nachricht für das ausstehende Ereignis "Benutzer erstellen" zum Beispiel folgendermaßen:

   CreateUserEvent.tmpl

   Unter "Identity Manager-Ereignisse" finden Sie eine Liste mit Ereignissen.

   Hinweis: Wenn Sie eine E-Mail-Vorlagendatei mit einem Dateinamen in einer anderen Sprache erstellen, sollte die Betriebssystemsitzung in einer Sprache ausgeführt werden, die den Zeichensatz unterstützt.

3. Ändern Sie die Nachrichtenvorlage nach Bedarf, wie im nächsten Abschnitt, Benutzerdefinierte E-Mail-Vorlagen (siehe Seite 408), beschrieben wird.

Benutzerdefinierte E-Mail-Vorlagen

Eine E-Mail-Vorlage ist eine dynamische Datei, die sowohl HTML als auch eingebettetes serverseitiges JavaScript unterstützt. Mithilfe einer Vorlage können Sie Variablenwerte in statischen Text einfügen, sodass fallspezifische Nachrichten aus einer einzelnen Vorlage generiert werden können.

Die gleiche Vorlage kann beliebig oft verwendet werden, um statische Textbausteine (zum Beispiel "wurde genehmigt") zusammen mit veränderlichem Text für einen bestimmten Kontext (zum Beispiel dem Namen des genehmigten Ereignisses) auszudrucken.

Beispiel einer Vorlage, um die Genehmigung eines Ereignisses zu melden:

```
<!-- Define the E-mail Properties --->
<%
   _to = _util.getNotifiers("ADMIN");
   _cc = "" ;
   _bcc = "";
   _subject = _eventContextInformation.getEventName() + " approved";
%>
<!--- Start of Body --->
<html>
<body text="Navy">
```

```
Ereignis: <b> <%=_eventContextInformation.getEventName()%> </b><br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
In <%=_eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%=_eventContextInformation.getSecondaryObjectName()%></b><br>
Status: <b>Genehmigt</b>
</body>
</html>
```

Hinweis: Die Identity Manager-Objekte "_util" und "_eventContextInformation", die im obigen Beispiel verwendet werden, werden unter E-Mail-Vorlagen-API beschrieben.

Wenn eine Genehmigung für das Ereignis "CreateUserEvent" generiert wird und der Benutzer John Jones in der HR-Abteilung der Organisation erstellt wird, könnte der Text der von der Genehmigungsvorlage generierten E-Mail-Benachrichtigung folgendermaßen aussehen:

```
Ereignis: CreateUserEvent
USER: John Jones
In ORGANIZATION: HR
Status: Genehmigt
```

In den folgenden Abschnitten werden die Syntax- und Identity Manager-Objekte beschrieben, die dynamische E-Mail-Nachrichten ermöglichen.

Vorlagen-Elemente

Identity Manager-E-Mail-Vorlagen unterstützen:

- Standardmäßige HTML-Tags.
- Serverseitiges JavaScript.
- Ein oder mehrere implizite Objekte, die Identity Manager für eine Instanz der Vorlage - d. h. eine E-Mail-Nachricht - verfügbar macht.
- Identity Manager-Tags, mit denen Sie JavaScript in die Vorlage einbetten, die Methoden in den impliziten Identity Manager-Objekten aufrufen und Variablenwerte in den statischen Text der Vorlage einfügen können.

Identity Manager-Tag-Erweiterungen

E-Mail-Vorlagen unterstützen die folgenden Tags:

<% %>

Bettet JavaScript in eine E-Mail-Vorlage ein.

<%= %>

Fügt einen Variablenwert in statischen Text ein.

Die Tags werden in den folgenden Abschnitten beschrieben.

<% %>

Mit diesem Tag können Sie JavaScript für die sequentielle Ausführung in eine E-Mail-Vorlage einbetten.

Sie können ein beliebiges JavaScript-Objekt innerhalb des eingebetteten JavaScript verwenden. Sie können auch implizite Identity Manager-Objektmethoden innerhalb des eingebetteten JavaScript aufrufen.

Mit dem folgenden Code wird zum Beispiel der Text der Genehmigungsvorlage geändert, die unter Benutzerdefinierte E-Mail-Vorlagen (siehe Seite 408) gezeigt wird. Mithilfe von JavaScript wird festgestellt, ob ein sekundäres Objekt am Ereignis beteiligt ist (zum Beispiel das Objekt ORGANISATION, wenn das primäre Objekt BENUTZER hinzugefügt wird). Wenn es kein sekundäres Objekt gibt, wird der Text bezüglich des sekundären Objekts aus der Nachricht weggelassen:

```
Ereignis: <b> <%=_eventContextInformation.getEventName()%> </b><br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
<%
var secondaryType =        _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
   template.add("In " + secondaryType + ": ");
   template.add("<b> "+_eventContextInformation.getSecondary
                                    ObjectName()+" </b><br>");
   }
%>
Status: <b>Genehmigt</b>
```

<%= %>

Mit diesem Tag können Sie einen Variablenwert in den statischen Text einfügen. Bei dem Wert kann es sich um Folgendes handeln:

- Eine Variable, die in einem zuvor ausgeführten JavaScript in der Vorlage definiert wurde, zum Beispiel:

```
<%
var secondaryType
=      _eventContextInformation.getSecondaryObjectTypeName();
...           // More JavaScript processing
%>
...           // More HTML
Das primäre Objekt wurde in <%=secondaryType%> erstellt.
```

- Ein Wert, der von einer Methode in einem impliziten Identity Manager-Objekt zurückgegeben wurde, zum Beispiel:

```
Ereignis <%=_eventContextInformation.getEventName()%> ist genehmigt.
```

E-Mail-Vorlagen-API

Wenn eine Nachricht aus einer Vorlage generiert wird, stellt Identity Manager die impliziten Objekte weiter unten für die Nachricht zur Verfügung. Mit diesen Objekten können Sie Informationen, die für eine Instanz spezifisch sind, in eine Nachricht einfügen, indem Sie Methoden in der E-Mail-Vorlage aufrufen.

Eine Vorlage kann die Methoden in den folgenden Objekte aufrufen:

- _contentType. Gibt den Inhaltstyp für die E-Mail an.
- _priority. Gibt die Priorität für die E-Mail an.
- _to. Fügt Empfänger im Feld "An" der Nachricht hinzu.
- _cc. Fügt Empfänger im Feld "CC" (Kopie senden an) der Nachricht hinzu.
- _bcc. Fügt Empfänger im Feld "BCC" (Blindkopie senden an) der Nachricht hinzu.
- _subject. Gibt den Betreff der E-Mail an.
- _encoding. Gibt die Kodierung für die E-Mail an.
- template. Ermöglicht das Hinzufügen einer Textzeichenfolge in einer Nachricht aus Zeilen mit JavaScript-Code.
- _util. Ein Hilfsprogrammobjekt.

- _eventContextInformation. Enthält Informationen zum Ereignis, das von der aktuellen Aufgabe generierte wurde, zum Beispiel Ereignisname und Genehmigungsstatus.
- _taskContextInformation. Enthält eine Sammlung von Informationen zur aktuellen Aufgabe, zum Beispiel Aufgabenname, Organisationsname und die einzelnen Ereignisse.

Diese Objekte werden in den folgenden Abschnitten erläutert.

_contentType

Gibt den Inhaltstyp für die E-Mail an.

Wenn mit der _contentType-Variable kein Inhaltstyp angegeben wird, wird der Standard-Inhaltstyp "text/html" verwendet.

Methoden: Keine.

Beispiel:

```
<% _contentType = "text/html"; %>
```

_priority

Gibt die Priorität für die E-Mail an. Geben Sie 0 für keine Priorität (Standard) und 1 für hohe Priorität an.

Methoden: Keine.

Beispiel:

```
<% _priority = "1"; %>
```

_to

Fügt Empfänger im Feld "An" der Nachricht hinzu.

Der Wert der _to-Variable ist eine JavaScript-Zeichenfolge. Mehrere Empfänger sind zulässig, aber die Zeichenfolge muss der JavaScript-Syntax entsprechen, die im folgenden Beispiel gezeigt wird.

Methoden: Keine.

Beispiel:

```
<%
_to =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
_cc = "" ;
_bcc = "" ;
_subject = "Ihr neues Kennwort ";
%>
```

Hinweis: Wenn E-Mails Teilnehmer darauf hinweisen, dass eine Aufgabe den Status "Ausstehend" hat und der Workflow-Steuerung unterliegt, sind die Adressen der Teilnehmer im _to-Objekt bereits enthalten. Sie können das _to-Objekt nicht in einer Vorlage für den Status "Ausstehend" verwenden.

_cc

Fügt Empfänger im Feld "CC" (Kopie senden an) der Nachricht hinzu.

Der Wert der _to-Variable ist eine JavaScript-Zeichenfolge. Mehrere Empfänger sind zulässig, aber die Zeichenfolge muss der JavaScript-Syntax entsprechen, die im folgenden Beispiel gezeigt wird.

Methoden: Keine.

Beispiel:

```
<%
_cc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
%>
```

_bcc

Fügt Empfänger im Feld "BCC" (Blindkopie senden an) der Nachricht hinzu.

In diesem Feld angegebene E-Mail-Adressen werden in der E-Mail nicht angezeigt.

Der Wert der _to-Variable ist eine JavaScript-Zeichenfolge. Mehrere Empfänger sind zulässig, aber die Zeichenfolge muss der JavaScript-Syntax entsprechen, die im folgenden Beispiel gezeigt wird.

Methoden: Keine.

Beispiel:

```
<%
_bcc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
%>
```

_subject

Gibt den Betreff der E-Mail an.

Methoden: Keine.

Beispiel:

```
<% _subject=_eventContextInformation.getEventName()+" approved";%>
```

_encoding

Gibt die Kodierung für die E-Mail an.

Wenn mit _encoding oder durch die LANG-Variable keine Kodierung angegeben wird, werden Zeichen in der E-Mail möglicherweise nicht richtig angezeigt. Legen Sie _encoding oder LANG auf das entsprechende Gebietsschema fest.

Methoden: Keine.

Beispiel:

```
<% _encoding = "UTF-8"; %>
```

_additionalHeaders

_additionalHeaders

Gibt zusätzliche E-Mail-Header-Attribute in der E-Mail-Vorlage an.

Sie müssen diesem Attribut eine HashMap() zuweisen. Die in der HashMap gespeicherten Namen und Werte müssen Zeichenfolgen sein.

Beispiel: Hinzufügen von benutzerdefinierten Header-Attributen

Im folgenden Beispiel wird gezeigt, wie zwei benutzerdefinierte Header-Attribute, "X-TCCCSWD" und "myheader", hinzugefügt werden:

```
<!-- Define the E-mail Properties --->
<%
_to = "siteadmin@ca.com";
_cc = "" ;
_bcc = "" ;
_subject = _eventContextInformation.getEventName() +" completed";
var additionalHeaders = new java.util.HashMap();
additionalHeaders.put("header_a","1");
additionalHeaders.put("header_b","foo");
_additionalHeaders = additionalHeaders;
%>
```

template

Ermöglicht das Hinzufügen einer Textzeichenfolge in einer Nachricht aus Zeilen mit JavaScript-Code (das heißt Zeilen innerhalb des <% %>-Tags). Die Zeichenfolge kann HTML-Tags, statischen Text und/oder Variablenwerte enthalten, die von Methoden in impliziten Identity Manager-Objekten zurückgegeben wurden.

Hinweis: Das Vorlagenobjekt wird nicht durch einen Unterstrich (_) eingeleitet.

Methode:

- add(String)

  Das Argument muss zu einer Zeichenfolge aufgelöst werden, einschließlich aller Methodenaufrufe in einem impliziten Identity Manager-Objekt. Im nachfolgenden Beispiel sehen Sie _eventContextInformation.getSecondaryObjectName().

Beispiel:

```
<%
var secondaryType =        _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
   template.add("In " + secondaryType + ": ");
   template.add("<b> "+_eventContextInformation.getSecondary
                                    ObjectName()+" </b><br>");
   }
%>
```

_util

Hilfsprogrammobjekt.

Methode:

- getNotifiers(String [,String])

  Gibt E-Mail-IDs basierend auf einer Benachrichtigungsregel zurück.

  Das erste Argument unterstützt die folgenden vordefinierten Benachrichtigungsregeln, die in Anführungszeichen eingeschlossen werden:

  - "ADMIN". Sendet die E-Mail an den Administrator, der die Aufgabe initiiert hat.
  - "USER". Sendet die E-Mail an den Benutzer im aktuellen Kontext.
  - "USER_MANAGER". Sendet die E-Mail an den Manager des Benutzers im aktuellen Kontext.

Sie können auch auf eine benutzerdefinierte Benachrichtigungsregel verweisen, die Sie mit der Benachrichtigungsregel-API erstellen. Weitere Informationen finden Sie im *Programmierhandbuch für Java*.

Das zweite Argument ist optional. Sie können es verwenden, um ein oder mehrere benutzerdefinierte Name/Wertepaare an eine benutzerdefinierte Benachrichtigungsregel zu übergeben. Trennen Sie jedes Name/Wertepaar mit einem Komma, und verwenden Sie das folgende Format:
`"name1=value1,name2=value2,..."`

Beispiele:

```
<%
_to = _util.getNotifiers("ADMIN");
_cc = "";
%>
<%
_to = _util.getNotifiers("MYRULE","type=loan,district=3");
_cc = "";
%>
```

Benachrichtigen des Managers eines Benutzers

Mit der USER_MANAGER-Benachrichtigungsregel können Sie eine E-Mail an den Manager eines jeden Benutzers senden. Identity Manager verwendet diese Regel in den E-Mail-Vorlagen, die die Zertifizierung von Benutzerberechtigungen unterstützen.

Hinweis: Die USER_MANAGER-Benachrichtigungsregel kann nur für Ereignisse oder Aufgaben verwendet werden, mit denen ein einzelner Benutzer erstellt oder verwaltet wird.

Da es verschiedene Methoden gibt, um eine Benutzer-/Manager-Beziehung innerhalb eines Benutzerverzeichnisses anzugeben, löst der Standardadapter für die Benachrichtigung des Benutzer-Managers diese Beziehung basierend auf einem im zweiten Parameter der getNotifiers()-Methode angegebenen Attributausdruck auf.

Beispiel:

```
<%
_to = _util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
_cc = "";
%>
```

Der Adapter für die Benachrichtigung des Benutzer-Managers unterstützt zwei Suchoptionen:

- managerattribute **=** **<***Manager AttributeName***>** - wobei das Benutzer-Objekt ein Attribut verwaltet, das den DN oder die Benutzer-ID des Benutzer-Managers angibt
- commonattribute **=** **<***AttributeName***>** - wobei der Benutzer und der Benutzer-Manager einen gemeinsamen Attributwert haben, zum Beispiel "Abteilung"

Sie konfigurieren diese Suchoptionen unter "Miscellaneous Properties" (Verschiedene Eigenschaften) für eine Umgebung in der Identity Manager-Management-Konsole.

So konfigurieren Sie die USER_MANAGER-Benachrichtigungsregel:

1. Wählen Sie in der Identity Manager-Management-Konsole "Identity Manager Environments" (Identity Manager-Umgebungen) aus. Wählen Sie dann die Umgebung aus, für die Sie die E-Mail-Benachrichtigung konfigurieren.
2. Wählen Sie "Advanced Settings" (Erweiterte Einstellungen) > "Miscellaneous Properties" (Verschiedene Eigenschaften).
3. Führen Sie auf der Seite "Miscellaneous Properties" die Konfigurationsschritte für die Suchoption aus, die Sie verwenden möchten:
   - So verwenden Sie die Suchoption "managerattribute=<Manager AttributeName>":
     a. Geben Sie im Feld "Eigenschaft" die Zeichenfolge "managerattribute" ein.
     b. Geben Sie im Feld "Wert" das Attribut ein, das den DN des Managers oder die Benutzer-ID speichert.
     c. Klicken Sie auf "Hinzufügen".
     d. Klicken Sie auf "Speichern".
   - So verwenden Sie die Suchoption "commonattribute=<AttributeName>":
     a. Geben Sie im Feld "Eigenschaft" die Zeichenfolge "commonattribute" ein.
     b. Geben Sie im Feld "Wert" das Attribut ein, das der Benutzer und der Benutzer-Manager gemeinsam haben.
     c. Klicken Sie auf "Hinzufügen".
     d. Geben Sie im Feld "Eigenschaft" die Zeichenfolge "ismanagerfilter" ein.

e. Geben Sie im Feld "Wert" einen Suchausdruck mithilfe der folgenden Syntax ein:

   <Attribut> <Operator> <Filter>

   Beispiel: Titel EQUALS Manager

f. Klicken Sie auf "Hinzufügen".

g. Klicken Sie auf "Speichern".

Sie können auch einen benutzerdefinierten Adapter schreiben und eigene Regeln für die Benachrichtigung des Managers eines Benutzers erstellen. Weitere Informationen finden Sie im *Programmierhandbuch für Java*.

_eventContextInformation

Enthält Informationen zum Ereignis, das von der aktuellen Aufgabe generierte wurde, zum Beispiel Ereignisname und Genehmigungsstatus. Diese Informationen werden als *Kontextinformationen* für das Ereignis bezeichnet.

Das _eventContextInformation-Objekt wird aus der ExposedEventContextInformation-Klasse in Paket "com.netegrity.imapi" erstellt.

Dieses Objekt ist für E-Mail-Nachrichten verfügbar, die auf Vorlagen mit den Status "Genehmigt", "Ausstehend" und "Abgelehnt" basieren. Weitere Informationen zu diesen Vorlagen finden Sie unter E-Mail-Vorlagen (siehe Seite 405).

Methoden: Alle folgenden Methoden geben eine Zeichenfolge zurück.

methode	Beschreibung
getAdminName()	Gibt den Namen der Person zurück, die die Aufgabe gesendet hat, die das Ereignis generiert hat. Veraltete Methode in CA IdentityMinder 5.6. Verwenden Sie eine der folgenden geerbten Methoden: ■ getAdministrator() ■ getAdminFriendlyName()
getApprovalStatus()	Gibt den Genehmigungsstatus des Ereignisses zurück. Einen dieser Werte: APPROVAL_STATUS_APPROVED APPROVAL_STATUS_REJECTED
getApprovalTime()	Gibt den Zeitpunkt zurück, zu dem das Ereignis genehmigt wurde.

methode	Beschreibung
getEventName()	Gibt den Namen des Ereignisses zurück. Eine Liste der Ereignisnamen finden Sie unter "CA IdentityMinder-Ereignisse".
getOrgName()	Gibt den Anzeigenamen der Organisation zurück, in der die Aufgabe ausgeführt wird. Veraltete Methode in CA IdentityMinder 5.6. Verwenden Sie die geerbte Methode "getObjectOrganizationFriendlyName()".
getPassword()	Wenn die primären Objekte vom Typ USER sind, wird das Kennwort des Benutzers zurückgegeben.
getPrimaryObjectTypeName()	Gibt den Typ des primären Objekts zurück. Zurückgegebene primäre Objekttypen: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER
getPrimaryObjectName()	Gibt den Namen des primären Objekts zurück, das vom Ereignis betroffen ist. Ein *primäres Objekt* ist das Objekt, das vom Ereignis direkt betroffen ist. Ein *sekundäres Objekt* ist ggf. das Objekt, an welches das primäre Objekt gebunden ist. Beispiel: ■ Der primäre Objekttyp für CreateUserEvent ist USER. Das sekundäre Objekt ist das Objekt, in dem der Benutzer erstellt wird - also ORGANIZATION. ■ Der primäre Objekttyp für CreateAdminRoleEvent ist ADMINROLE. Dieses Objekt ist nicht an andere Objekte gebunden, sodass kein sekundäres Objekt vorhanden ist. Bei einem primären Objekt des Typs USER könnte mit getPrimaryObjectName() John Jones zurückgegeben werden.

methode	Beschreibung
getSecondaryObjectTypeName()	Gibt den Objekttyp zurück, wenn sich das Ereignis auf ein sekundäres Objekt ausgewirkt hat. Zurückgegebene sekundäre Objekttypen: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER
getSecondaryObjectName()	Gibt den Objektnamen zurück, wenn sich das Ereignis auf ein sekundäres Objekt ausgewirkt hat. Weitere Informationen zu primären und sekundären Objekten finden Sie unter "getPrimaryObjectName()". Bei einem sekundären Objekt des Typs ORGANIZATION könnte die getSecondaryObjectName()-Methode HR zurückgeben.

Hinweis: Die Methoden in "_eventContextInformation" werden über die ExposedEventContextInformation-Schnittstelle angegeben. Da ExposedEventContextInformation Methoden in der CA IdentityMinder-Kern-API erbt, können auch diese Methoden mit _eventContextInformation aus einer E-Mail-Vorlage aufgerufen werden - zusammen mit den Methoden in der Tabelle oben. Weitere Informationen zu diesen geerbten Methoden finden Sie unter Zusätzliche Methoden (siehe Seite 425).

Beispiel: E-Mail-Benachrichtigung über ein Ereignis mit dem Status "Ausstehend":

```
<%
_cc = "" ;
_bcc = "";
_subject = _eventContextInformation.getEventName() +
                                                " Approval Request";
%>
<!--- Start of Body --->
<html>
<body text="Navy">

Das folgende Element wurde Ihrer Arbeitsliste zur Genehmigung hinzugefügt:
<br><br><br>
Ereignis: <b><%=_eventContextInformation.getEventName()%></b> <br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
In <%=_eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%=_eventContextInformation.getSecondaryObjectName()%></b><br>
</body>
</html>
```

Möglicher E-Mail-Text:

```
Vom: lsmith@security.com [mailto:lsmith@security.com]
An: vimperioso@security.com
Betreff: CreateUserEvent-Genehmigungsanfrage

Das folgende Element wurde Ihrer Arbeitsliste zur Genehmigung hinzugefügt:

Ereignis: CreateUserEvent
USER: Richard Ferrigamo
In ORGANIZATION: Mortgages & Loans
```

Hinweis: Der Wert des Felds "Von" wird aus der email.properties-Datei abgeleitet. Um den Wert zu ändern, bearbeiten Sie die folgende Datei:

<*iam_im.ear*>\config\com\netegrity\config\email.properties

wobei <*iam_im.ear*> das Installationsverzeichnis von CA IdentityMinder in der Anwendungsserverdomäne ist, zum Beispiel:

Für WebLogic:

<*WebLogic_Basisverzeichnis*>\user_projects\<Domäne>\applications\iam_im.ear

Für JBoss:

<*Identity Manager_Basisverzeichnis*>\jboss-3.2.2\server\default\deploy\iam_im.ear

Für WebSphere:

<*im_admin_tools_dir* >\WebSphere-ear\iam_im.ear

Um zusätzliche Informationen zum Benutzer, der vom Ereignis betroffen ist, in der E-Mail im vorherigen Beispiel hinzuzufügen, fügen Sie Text hinzu, der in etwa dem Folgenden entspricht:

```
<% user = _eventContextInformation.getEvent().getUser(); %>
<b>Benutzerinformationen:</b><br>
Nachname: <b><%=user.getAttribute("%LAST_NAME%")%></b><br>
Vorname: <b><%=user.getAttribute("%FIRST_NAME%")%></b><br>
Vollständiger Name: <b><%=user.getAttribute("%FULL_NAME%")%></b><br>
E-Mail: <b><%=user.getAttribute("%EMAIL%")%></b><br>
Organization Membership (Organisationsmitgliedschaft):
<b><%=user.getAttribute("%ORG_MEMBERSHIP%")%></b><br>
```

Möglicher E-Mail-Text:

Vom: lsmith@security.com [mailto:lsmith@security.com]
An: vimperioso@security.com
Betreff: CreateUserEvent-Genehmigungsanfrage

Das folgende Element wurde Ihrer Arbeitsliste zur Genehmigung hinzugefügt:

Ereignis: **CreateUserEvent**
USER: **Richard Ferrigamo**
In ORGANIZATION: **Mortgages & Loans**
Benutzerinformationen:
Nachname: Ferrigamo
Vorname: Richard
Vollständiger Name: Richard Ferrigamo
E-Mail: rferrigamo@mybank.org
Organization Membership (Organisationsmitgliedschaft): **Mortgages & Loans**

_taskContextInformation

Enthält eine Sammlung von Informationen zur aktuellen Aufgabe, zum Beispiel Aufgabenname, Organisationsname und die einzelnen Ereignisse. Diese Informationen werden als *Kontextinformationen* für die Aufgabe bezeichnet.

Dieses Objekt ist für E-Mail-Nachrichten verfügbar, die auf Vorlagen für den Status "Abgeschlossen" basieren. Weitere Informationen zu dieser Vorlage finden Sie unter E-Mail-Vorlagen (siehe Seite 405).

Methoden: Alle nachfolgenden Methoden geben eine Zeichenfolge zurück - abgesehen von der Methode getExposedEventContexts(), die einen Java-Vektor zurückgibt.

methode	Beschreibung
getAdminName()	Gibt den Namen der Person zurück, die die Aufgabe sendet. Veraltete Methode in Identity Manager 5.6. Verwenden Sie eine der folgenden geerbten Methoden: ■ getAdministrator() ■ getAdminFriendlyName()
getExposedEventContexts()	Gibt einen Java-Vektor von allen der Aufgabe zugeordneten Ereignisse zurück. Jedes Objekt im Vektor ist ein Ereigniskontextobjekt. Mit den in "_eventContextInformation" aufgeführten Methoden können Sie Kontextinformationen für ein bestimmtes Ereignisobjekt abrufen. Das zurückgegebene Objekt ist ein standardmäßiges Java-Vektor-Objekt. Sie können jede der Methoden des Vektor-Objekts verwenden, zum Beispiel get() and size(), um die Elemente im Vektor zu verwalten.
getOrgName()	Gibt den Namen der Organisation zurück, in der die Aufgabe ausgeführt wird. Veraltete Methode in Identity Manager 5.6. Verwenden Sie die geerbte Methode "getObjectOrganizationFriendlyName()".
getTaskName()	Gibt den Namen der Aufgabe zurück, die ausgeführt wird. Veraltete Methode in Identity Manager 5.6. Verwenden Sie eine der folgenden geerbten Methoden: ■ getAdminTask() ■ getTaskFriendlyName()

Hinweis: Die Methoden in "_taskContextInformation" werden über die ExposedTaskContextInformation-Schnittstelle angegeben. Da ExposedTaskContextInformation Methoden in der Identity Manager-Kern-API erbt, können auch diese Methoden mit _taskContextInformation aus einer E-Mail-Vorlage aufgerufen werden - zusammen mit den Methoden in der Tabelle oben. Weitere Informationen zu diesen geerbten Methoden finden Sie unter Zusätzliche Methoden (siehe Seite 425).

Beispiel: Text einer E-Mail-Benachrichtigungsvorlage für eine Kennwortänderung:

```
<%
var imsEventContexts
=              _taskContextInformation.getExposedEventContexts();
if(imsEventContexts != null)
   {
   for(var i=0;i<imsEventContexts.size();i++)
      {
      var eventContext = imsEventContexts.get(i);
      template.add("Hi "+
eventContext.getPrimaryObjectName()
           + ",");
      template.add("<br>Ihr neues Kennwort lautet: <b>"+
                              eventContext.getPassword());</br>
      template.add("<hr>");
      }
   }
%>
```

Möglicher E-Mail-Text:

Hallo Victor Imperioso,
Ihr neues Kennwort lautet: LFH7F1226

Zusätzliche Methoden

Die Methoden in "_taskContextInformation" und "_eventContextInformation" werden über die Identity Manager-Objekte "ExposedTaskContextInformation" bzw. "ExposedEventContextInformation" angegeben.

Diese Objekte erben Methoden in der Identity Manager-Kern-API. Folglich sind die geerbten Methoden auch für "_taskContextInformation" und "_eventContextInformation" verfügbar.

Die folgenden vom TaskInfo-Objekt geerbten Methoden sind für eine E-Mail-Vorlage besonders nützlich:

- getAdministrator(). Ruft ein Benutzerobjekt für den Administrator ab, der die aktuelle Aufgabe ausführt.
- getAdminTask(). Ruft ein Admin-Aufgabenobjekt für die aktuelle Aufgabe ab.

Mithilfe dieser abgerufenen Objekte können Sie für einen Administrator oder eine Aufgabe spezifische Informationen in eine E-Mail einfügen. Beispiel:

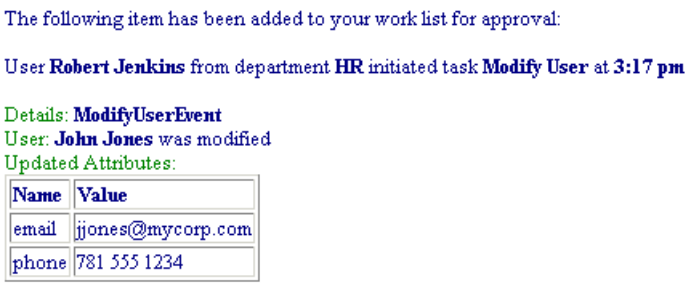
```
<!-- Define the E-mail Properties --->

<%
   _cc = "" ;
   _bcc = "" ;
   _subject = _eventContextInformation.getEventName() +
                                                 " Approval Request";
%>
<!--- Start of Body --->
<html>
<body text="Navy">

The following item has been added to your work list for approval:<br>
<br>
User <b><%= _eventContextInformation.getAdministrator().
               getAttribute(Packages.com.netegrity.llsdk6.imsapi.
                managedobject.User.PROPERTY_FRIENDLY_NAME)%> </b>
               from department <b><%= _eventContextInformation.
               getAdministrator().getOrg(null).getFriendlyName()
               %></b> initiated task <b><%= _eventContextInformation.
               getAdminTask().getFriendlyName() %></b>at
<b><%=                _eventContextInformation.getSessionCreateTime() %></b>
<br><br>
<font color="green">Details: </font><b><%=_eventContextInformation.
                                          getEventName()%></b><br>
<font color="green"><%=_eventContextInformation.
                               getPrimaryObjectTypeName()%>:</font>
<b><%=_eventContextInformation.getPrimaryObjectName()%></b>
                                                        was modified
<br>
<font color="green">Aktualisierte Attribute:</font>
<table border="1">
<tr>
  <td><b>Name</b></td>
  <td><b>Wert</b></td>
</tr>
```

```
<%
   var event = _eventContextInformation.getEvent();
   if(event instanceof Packages.com.netegrity.imapi.UserEvent) {
      var user = event.getUser();
      var attributes = user.getAttributes().keys();
      while(attributes.hasMoreElements()) {
         var attr = attributes.nextElement();
         var value = user.getAttribute(attr);
         if(user.hasAttributeChanged(attr)) {
            template.add("<tr><td> " + attr +"</td>");
            template.add("<td>" + value +"</td></tr>");
         }
      }
   }
%>
</table>
<br>
</body>
</html>
```

Möglicher E-Mail-Text:


The following item has been added to your work list for approval:

User **Robert Jenkins** from department **HR** initiated task **Modify User** at **3:17 pm**

Details: **ModifyUserEvent**
User: **John Jones** was modified
Updated Attributes:

Name	Value
email	jjones@mycorp.com
phone	781 555 1234

Weitere Informationen zu den geerbten Methoden, die für die E-Mail-Vorlagen-API verfügbar sind, finden Sie unter den Objekten "ExposedTaskContextInformation" und "ExposedEventContextInformation" in der Identity Manager Javadoc.

Java-Standardausgabestream

Eine E-Mail-Nachricht kann Aufrufe an den Java-Standardausgabestream auch von einem JavaScript-Tag (<% %>) aus durchführen. Zum Beispiel sendet der folgende Aufruf die Meldung "Fertig" an die Serverkonsole:

```
<%
...       // JavaScript processing
out.println("Fertig.");
%>
```

Javadoc-Referenz

Weitere Informationen zu den Objekten "ExposedTaskContextInformation" und "ExposedEventContextInformation", einschließlich der Methoden, die sie von der Identity Manager-Kern-API erben, finden Sie in der Identity Manager Javadoc.

Die Javadoc-Seiten sind in einer HTML-Version des Programmierhandbuchs für Java integriert, das im Identity Manager-Bookshelf verfügbar ist.

Bereitstellung von E-Mail-Vorlagen

Bevor CA IdentityMinder eine E-Mail sendet, sucht die Anwendung im folgenden Stammverzeichnis auf Ihrem Anwendungsserver nach Vorlagen, um die E-Mail zu generieren:
iam_im.ear\custom\emailTemplates

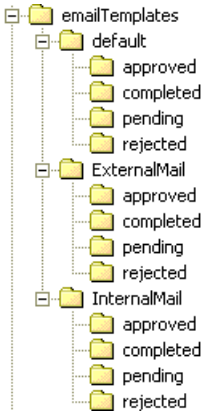
Die in diesem Stamm bereitgestellten E-Mail-Vorlagen sind in Vorlagensätzen mit der gleichen Verzeichnisstruktur enthalten - das heißt, dass es in jedem Satz die Verzeichnisse "approved", "completed", "pending" und "rejected" gibt.

Vorlagensätze

Sie können unter "emailTemplates" mehrere Sätze von E-Mail-Vorlagen bereitstellen. Zum Beispiel wird bei der Installation der folgende Satz von E-Mail-Vorlagen unter "iam_im.ear\custom\emailTemplates" erstellt:

```
Standard\Genehmigt
Standard\Abgeschlossen
Standard\Ausstehend
Standard\Abgelehnt
```

Das standardmäßige E-Mail-Vorlagensatz enthält die installierten Vorlagen, die unter E-Mail-Vorlagen (siehe Seite 405) beschrieben werden. Sie können im Standardsatz benutzerdefinierte Vorlagen hinzufügen. Sie können auch andere Sätze von E-Mail-Vorlagen in Verzeichnisstrukturen bereitstellen, die Sie auf der gleichen Ebene wie den Standardsatz definieren. Zum Beispiel könnte "iam_im.ear\custom" die folgenden bereitgestellten E-Mail-Vorlagen enthalten:



Hinweis: Weitere Informationen dazu, wie CA IdentityMinder eine bestimmte E-Mail-Vorlage innerhalb eines Vorlagensatzes auswählt, finden Sie unter Vorlagenverzeichnisse (siehe Seite 407).

Festlegen eines Vorlagensatzes für eine Umgebung

Wenn Sie E-Mail für eine Identity Manager-Umgebung konfigurieren, legen Sie den E-Mail-Vorlagensatz fest, den Sie für diese Umgebung verwenden möchten. Weitere Informationen zum Konfigurieren von E-Mail für eine Identity Manager-Umgebung finden Sie im *CA Identity Manager-Konfigurationshandbuch*.

Vorlagennamen

Die Verzeichnisse in einem benutzerdefinierten Vorlagensatz sollten Standardvorlagen enthalten, die den gleichen Namen wie die im Standardvorlagensatz installierten Vorlagen haben. Die Standardnamen sind unter E-Mail-Vorlagen (siehe Seite 405) aufgelistet. Identity Manager verwendet die Standardvorlagen, wenn keine andere Vorlage mit einem Namen gefunden wird, der mit der Aufgabe oder dem Ereignis übereinstimmt, die bzw. das ausgeführt wird.

Optional können Sie zusätzliche Vorlagen in einem oder mehreren Verzeichnissen in einem Vorlagensatz hinzufügen, wenn eine E-Mail aus einer bestimmten Vorlage generiert werden soll. Vorgehensweise:

- Weisen Sie der Vorlage den Namen der Aufgabe oder des Ereignisses zu, für die bzw. das die E-Mail generiert wird.
- Legen Sie die Vorlage in dem Verzeichnis ab, das der Aufgabe oder dem Ereignis zugeordnet ist, für die bzw. das die E-Mail generiert wird.

Wenn E-Mails zum Beispiel aus einer bestimmten Vorlage generiert werden sollen, wenn ein CreateUserEvent abgelehnt wird, legen Sie im Verzeichnis "Abgelehnt" des Vorlagensatzes der Umgebung eine Vorlage mit dem Namen "CreateUserEvent.tmpl" ab.

Kapitel 14: Berichterstellung

Dieses Kapitel enthält folgende Themen:

Übersicht (siehe Seite 431)
Bericht-Prozess (siehe Seite 433)
So führen Sie einen Snapshot-Bericht aus (siehe Seite 434)
So führen Sie einen Nicht-Snapshot-Bericht aus (siehe Seite 449)
Festlegen von Berichtsoptionen (siehe Seite 455)
So können Sie einen benutzerdefinierten Snapshot-Bericht erstellen und ausführen (siehe Seite 456)
Fehlerbehebung (siehe Seite 470)

Übersicht

Innerhalb von CA IdentityMinder können Sie zwei verschiedene Typen von Berichten ausführen:

- Snapshot-Berichte - Beinhalten Daten aus der Snapshot-Datenbank, die Informationen aus dem CA IdentityMinder-Objektspeicher und dem CA IdentityMinder-Benutzerspeicher enthalten. Ein Beispiel eines Snapshot-Berichtes ist der Bericht über Benutzerprofile. Sie definieren mit Hilfe der Snapshot-Definitionen, die die aufzunehmenden Informationen angeben, welche Daten der Snapshot-Datenbank hinzugefügt werden.
- Nicht-Snapshot-Berichte - Beinhalten Daten aus anderen Datenquellen, wie z. B. der Audit-Datenbank. Zu Identity Manager gehören beispielsweise Standard-Audit-Berichte. (In der Benutzerkonsole führen diese Berichte das Präfix "Audit - " in ihrem Namen). Standardmäßig bietet CA IdentityMinder nur Audit-Berichte an, Sie können jedoch Ihre eigenen, benutzerdefinierten Berichte erstellen, die Daten aus jeder beliebigen Datenquelle wie Workflow- oder Aufgaben-Persistenz-Datenbanken enthalten können.

Jeder Bericht in CA IdentityMinder muss zunächst konfiguriert werden, bevor er ausgeführt werden kann. Die Konfigurationsschritte hängen vom Typ des Berichts ab, den Sie ausführen möchten.

Bei Snapshot-Berichten müssen folgende Schritte durchgeführt werden:

1. Erstellen Sie eine Snapshot-Definitionsdatei und definieren Sie, welche Daten der Snapshot-Datenbank hinzugefügt werden sollen.
2. Erfassen Sie die Snapshot-Daten für den Bericht.

3. Ändern Sie die Berichtsaufgabe in CA IdentityMinder und führen Sie die folgenden Aktionen durch:
   a. Weisen Sie der Aufgabe eine Snapshot-Definition zu.
   b. Fügen Sie der Aufgabe das Verbindungsobjekt "rptParamConn" hinzu.
4. Fordern Sie den Bericht mittels einer der folgenden Methoden an:
   - Bericht sofort ausführen
   - Ausführung des Berichts planen
5. Zeigen Sie den Bericht in der Benutzerkonsole an.

Bei Nicht-Snapshot-Berichten müssen folgende Schritte durchgeführt werden:

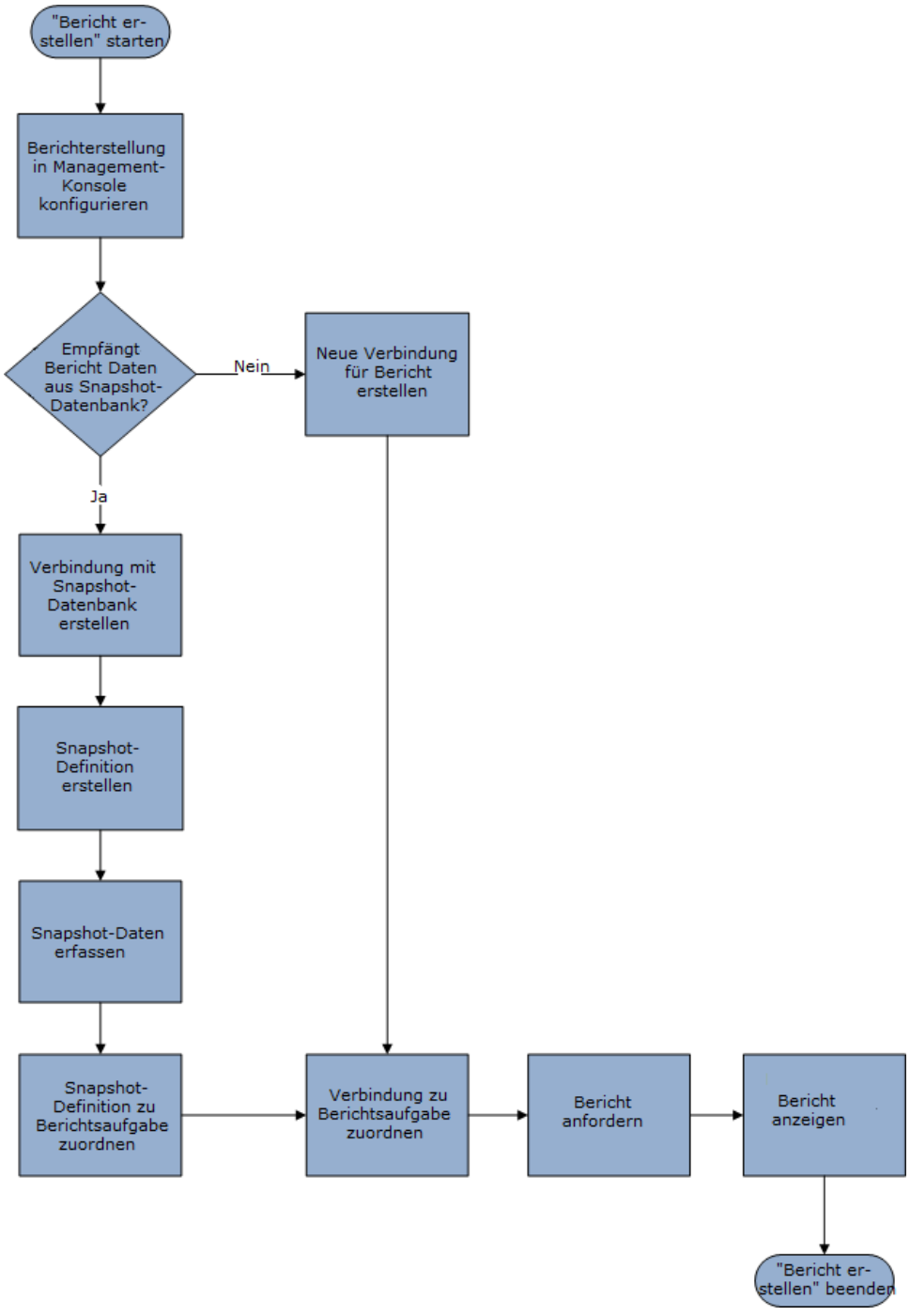
1. Erstellen Sie ein Verbindungsobjekt mit der Datenquelleninformation für den Bericht.
2. Ändern Sie die Berichtsaufgabe in CA IdentityMinder und fügen Sie der Aufgabe das Verbindungsobjekt hinzu.
3. Fordern Sie den Bericht mittels einer der folgenden Methoden an:
   - Bericht sofort ausführen
   - Ausführung des Berichts planen
4. Zeigen Sie den Bericht in der Benutzerkonsole an.

Nach Abschluss der anfänglichen Konfiguration Ihres Berichts können Sie ihn in CA IdentityMinder anfordern. Sie können einen Bericht sofort ausführen oder seine Ausführung zu einem späteren Zeitpunkt planen. Sie können für Ihren Bericht in CA IdentityMinder auch einen Plan mit wiederkehrenden Ausführungen erstellen.

Schließlich können Sie den Bericht von der Benutzerkonsole aus anzeigen oder ihn in verschiedene Formate exportieren.

Bericht-Prozess

Die folgende Grafik veranschaulicht den Prozess, der zum Ausführen und Anzeigen von Berichten erforderlich ist:



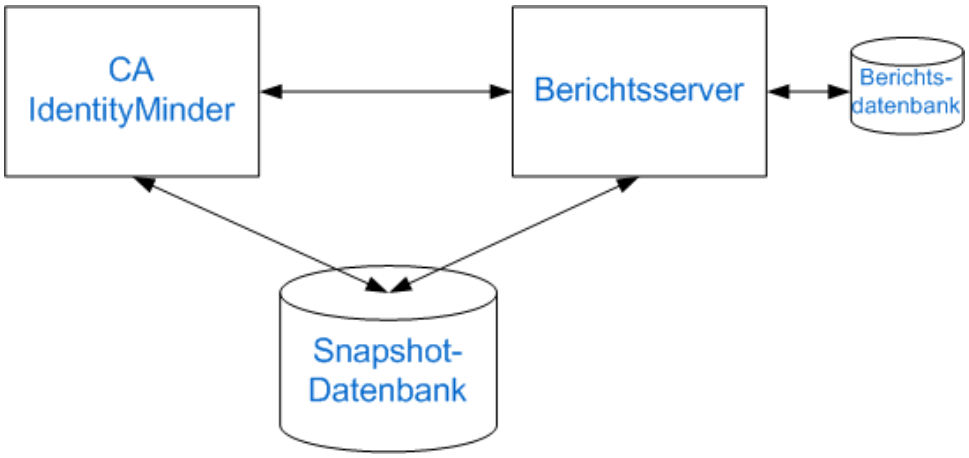
So führen Sie einen Snapshot-Bericht aus

CA IdentityMinder-Berichte ermöglichen die Anzeige des aktuellen Status einer CA IdentityMinder-Umgebung. Anhand dieser Informationen können Sie die Konformität mit internen Geschäftsrichtlinien oder externen Vorschriften gewährleisten.

CA IdentityMinder-Berichte werden aus Managementdaten generiert, die die Beziehung zwischen Objekten in einer CA IdentityMinder-Umgebung beschreiben. Managementdaten können Folgendes enthalten:

- Profilattribute der Benutzer
- Eine Liste der Rollen, die eine bestimmte Aufgabe enthalten
- Die Mitglieder einer Rolle oder Gruppe
- Die Regeln, die eine Rolle ausmachen

In CA IdentityMinder benötigt das Berichts-Setup die folgenden drei größeren Komponenten:



Hinweis: Die Snapshot-Datenbank in dieser Abbildungsgrafik könnte auch die Audit-Datenbank oder Workflow-Datenbank sein.

Berichtsserver

Auch bekannt als CA Business Intelligence generiert dieser Server Berichte, die direkt mit CA IdentityMinder und der Snapshot-Datenbank kommunizieren.

Berichtsdatenbank

Die Datenbank, in der CA-Berichtsserver (Business Objects) eigene Daten speichern.

CA IdentityMinder

CA IdentityMinder ermöglicht es Ihnen, CA IdentityMinder-Objektdaten in die Berichtsdatenbank zu exportieren.

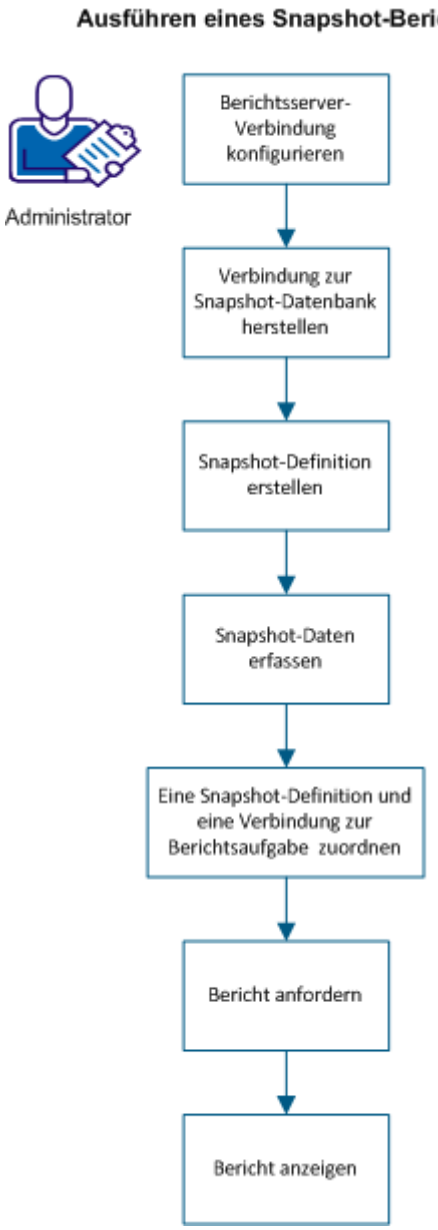
Snapshot-Datenbank

Eine separate Datenbank, die die Snapshot-Daten der Objekte in CA IdentityMinder enthält

Wichtig! Der Berichtsserver verwendet Business Objects Enterprise. Wenn Sie bereits einen Berichtsserver in Ihrer Umgebung haben und diesen mit CA IdentityMinder verwenden möchten, dann ist CA Business Intelligence 3.2 SP5 die minimale Version, die von CA IdentityMinder benötigt wird.

Ein Snapshot-Bericht enthält Daten aus der Snapshot-Datenbank, die Informationen aus dem CA IdentityMinder-Objektspeicher und dem CA IdentityMinder-Benutzerspeicher enthalten. Ein Beispiel eines Snapshot-Berichtes ist der Bericht über Benutzerprofile. Sie definieren mithilfe der Snapshot-Definitionen, die die aufzunehmenden Informationen angeben, welche Snapshot-Daten der Snapshot-Datenbank hinzugefügt werden.

Folgende Grafik veranschaulicht den Prozess für die Ausführung eines Snapshot-Berichts:



Um den Snapshot-Bericht auszuführen, führen Sie folgende Schritte aus:

1. Konfigurieren Sie die Berichtsserver-Verbindung (siehe Seite 450).
2. Erstellen Sie eine Snapshot-Datenbankverbindung.
3. Erstellen Sie eine Snapshot-Definition.
4. Erfassen Sie die Snapshot-Daten.
5. Weisen Sie der Berichtsaufgabe eine Snapshot-Definition und eine Verbindung zu.
6. Fordern Sie einen Bericht an (siehe Seite 446).

7. Zeigen Sie den Bericht an (siehe Seite 448).

Berichtsserver-Verbindung konfigurieren

Konfigurieren Sie die Verbindung zwischen CA IdentityMinder und dem Berichtsserver.

Hinweis: Wir empfehlen, dass für alle Systeme, die an der Berichterstellung beteiligt sind, dieselbe Zeitzone und Uhrzeit festgelegt wird.

So konfigurieren Sie die Berichterstellung

1. Klicken Sie in der Benutzerkonsole auf "System", "Berichterstellung", "Berichtsserver-Verbindung".
2. Geben Sie die Einstellungen für den Berichtsserver ein. Beachten Sie Folgendes:
   - Hostname und Port - Hostname und HTTP-URL-Portnummer des Systems, in dem der Berichtsserver installiert ist.
   - Berichtsordnername – Speicherort der Standardberichte für CA IdentityMinder.
   - Benutzer-ID – Benutzer, der für den Berichtsserver erstellt wurde.
   - Kennwort – Kennwort für den im Berichtsserver erstellten Benutzer.
   - Sichere Verbindung – Aktivieren Sie das Kontrollkästchen, um eine SSL-Verbindung (Secure Sockets Layer) zwischen CA IdentityMinder und Berichtsserver zu aktivieren.

     Hinweis: Bevor Sie das Kontrollkästchen "Sichere Verbindung" aktivieren, überprüfen Sie, dass Sie das Zertifikat vom BOServer installiert haben. Weitere Informationen darüber, wie Sie SSL richtig konfigurieren, finden Sie im Kapitel "Berichtsserver-Installation" im *Installationshandbuch*.
   - Webserver – Für Tomcat auf Nicht-IIS gesetzt
3. Klicken Sie auf "Verbindung testen", um die Verbindung zu überprüfen.
4. Klicken Sie auf "Senden".

Die Berichtsverbindung ist hergestellt.

Erstellen einer Snapshot-Datenbankverbindung

CA IdentityMinder muss wissen, wohin die Snapshot-Daten exportiert werden sollen. Stellen Sie zwischen CA IdentityMinder und der Snapshot-Datenbank eine Datenbankverbindung her.

So erstellen Sie eine Snapshot-Datenbankverbindung

1. Navigieren Sie in der Benutzerkonsole zu "Berichte", "Snapshot-Aufgaben", "Verbindung zur Snapshot-Datenbank verwalten" und "Verbindung zur Snapshot-Datenbank herstellen".
2. Erstellen Sie die neue Snapshot-Datenbankverbindung, indem Sie alle erforderlichen Felder ausfüllen.
3. Klicken Sie auf "Senden".

   Es wird eine neue Snapshot-Datenbank-Verbindung erstellt.

Erstellen einer Snapshot-Definition

Ein Snapshot spiegelt den Status von Objekten in CA IdentityMinder zu einer bestimmten Zeit wider. Sie verwenden diese Snapshot-Daten, um einen Bericht zu erstellen. Um CA IdentityMinder-Objektdaten zu erfassen, erstellen Sie eine Snapshot-Definition, die die Daten zur Snapshot-Datenbank exportiert. Mithilfe der Snapshot-Definition definieren Sie die Regeln, um Benutzer, Endpunkte, Admin-Rollen, Bereitstellungsrollen, Gruppen und Organisationen zu laden.

Gehen Sie wie folgt vor:

1. Navigieren Sie in der Benutzerkonsole zu "Berichte", "Snapshot-Aufgaben", "Snapshot-Definitionen verwalten" und "Snapshot-Definition erstellen".
2. Erstellen oder kopieren Sie ein Objekt vom Typ Snapshot.
3. Klicken Sie auf "OK".
4. Füllen Sie in der Registerkarte "Profil" die folgenden Felder aus, um das Profil einer Snapshot-Definition zu erstellen:

   Snapshot-Definitionsname

   Identifiziert den eindeutigen Namen für die Snapshot-Definition.

   Snapshot-Definitionsbeschreibung

   Zeigt alle zusätzlichen Informationen an, mit denen Sie den Snapshot beschreiben möchten.

   Aktiviert

   Gibt an, dass CA IdentityMinder basierend auf der aktuellen Snapshot-Definition zur geplanten Zeit einen Snapshot erstellt.

   Hinweis: Falls diese Option nicht ausgewählt ist, wird die Snapshot-Definition nicht zur geplanten Zeit erfasst. Darüber hinaus wird die Snapshot-Definition nicht im Fenster "Snapshot-Daten erfassen" aufgeführt.

   Anzahl der zurückgehaltenen Snapshots

   Gibt die Anzahl der erfolgreichen Snapshots an, die in der Snapshot-Datenbank beibehalten werden.

   Hinweis: Wenn Sie in diesem Feld keinen Wert angeben, speichert CA IdentityMinder eine unbegrenzte Anzahl von Snapshots.
5. Wählen Sie in der Registerkarte "Snapshot-Richtlinien" die Objekte aus, die sich auf die zu exportierenden Richtlinien beziehen.
6. Wählen Sie auf der Registerkarte "Rolleneinstellungen" eine oder mehrere Rollenkomponenten und verfügbare Attribute zum Exportieren des Snapshot aus.

   Hinweis: In der Registerkarte "Snapshot-Richtlinien", wenn Sie "Zugriffsrolle", "Admin-Rolle" oder "Bereitstellungsrolle" auswählen, wählen Sie die Attribute in der Registerkarte "Rolleneinstellungen" aus.

7. Wählen Sie auf der Registerkarte "Benutzerattributdetails" einen oder mehrere Benutzerattribute für den zu exportierenden Snapshot aus.

   Hinweis: Wenn Sie in der Registerkarte "Snapshot-Richtlinien" nur das Benutzerobjekt auswählen, werden standardmäßig alle zu den Benutzerattributen zugehörigen Daten exportiert.

8. Wählen Sie in der Registerkarte "Endpunktkontoattribute" ein oder mehrere Kontoattribute eines Endpunkttyps aus.

   Hinweis: Für einen ausgewählten Endpunkttyp werden standardmäßig alle auf die Endpunktkontoattribute bezogenen Daten exportiert. Um auf ein bestimmtes Attribut bezogene Daten zu erfassen, wählen Sie das entsprechende Attribut aus. Weitere Informationen für das Auswählen von Attributen, die notwendig sind, um einen Endpunkttyp zu exportieren, finden Sie im Abschnitt "Standardberichte" im *Konfigurationshandbuch*.

9. (Optional) Aktivieren Sie das Kontrollkästchen "Verwaiste Konten exportieren", um Endpunkt-Benutzerkonten ohne globalen Benutzer auf dem Bereitstellungsserver einzuschließen.

   Hinweis: Um Berichtsdaten für nicht standardmäßige, nicht standardmäßige Trend-Berichte und Berichte zu verwaisten Konten zu exportieren, wählen Sie das Attribut "Ausnahmenkonto" und das Kontrollkästchen "Verwaiste Konten exportieren" aus.

10. Klicken Sie auf "Senden".

    CA IdentityMinder ist so konfiguriert, dass Snapshots der Objekte erstellt werden, die in der Snapshot-Definition festgelegt sind.

Nachdem Sie nun eine Snapshot-Definition erstellt haben, können Sie sofort Snapshot-Daten erfassen oder den Snapshot-Datenexport zu einem späteren Zeitpunkt planen. Im Thema Erfassen von Snapshot-Daten (siehe Seite 442) erhalten Sie weitere Informationen.

Weitere Informationen:

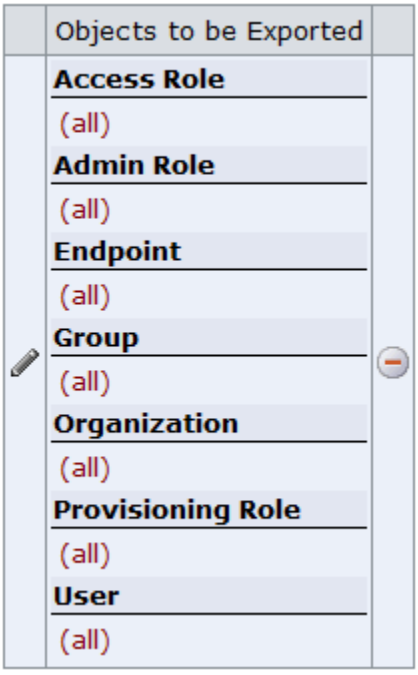
Registerkarte "Wiederholungen" (siehe Seite 443)

Beispiel: Erstellen einer Snapshot-Definition für Benutzerberechtigungsdaten

Das folgende Beispiel veranschaulicht den Prozess zum Erstellen einer Snapshot-Definition für einen Bericht zu Benutzerberechtigungen:

1. Navigieren Sie in der Benutzerkonsole zu "Berichte", "Snapshot-Aufgaben", "Snapshot-Definitionen verwalten" und "Snapshot-Definition erstellen".
2. Wählen Sie "Neues Objekt des Typs "Snapshot" erstellen" aus.
3. Geben Sie den Namen der Snapshot-Definition, eine Beschreibung und die Anzahl der beibehaltenen Snapshots ein.
4. Klicken Sie auf der Registerkarte "Snapshot-Richtliniendefinition" auf "Hinzufügen".

   Wählen Sie in der Drop-down-Liste den Benutzer und dann die Option "Alle" aus. Fügen Sie dementsprechend "Endpunkt", "Bereitstellungsrolle", "Admin-Rolle", "Zugriffsrolle", "Organisation" und "Gruppe", wie in der folgenden Grafik angezeigt, hinzu:



5. Aktivieren Sie auf der Registerkarte "Rolleneinstellungen" alle Kontrollkästchen für Benutzerrollen.
6. Wählen Sie auf der Registerkarte "Benutzerattribute" die erforderlichen Attribute aus der Liste "Verfügbare Werte" aus, und verschieben Sie sie in die Liste "Derzeitige Werte".
7. Klicken Sie auf "Senden".

Snapshots verwalten

CA IdentityMinder ermöglicht Ihnen das Anzeigen, Ändern und Löschen Ihrer Snapshot-Definitionen. Wenn Sie eine Snapshot-Definition anzeigen oder ändern, werden die Registerkarten "Profil" und "Wartung" angezeigt. Die Registerkarte "Wartung" wird erst angezeigt, nachdem ein Snapshot zum ersten Mal erfasst wurde. Auf der Registerkarte "Wartung" können Sie Ihre Snapshots löschen (auch wenn der Status des Snapshots "Fehlgeschlagen" lautet).

Wenn Sie eine Snapshot-Definition anzeigen, ändern oder löschen möchten , wechseln Sie zu "Berichte", "Snapshot-Aufgaben", "Snapshot-Definitionen verwalten", und klicken Sie auf die Aufgabe, die Sie ausführen möchten.

Hinweis: Wenn eine Snapshot-Definition zum Exportieren von Daten in die Snapshot-Datenbank verwendet wird, kann sie nicht gelöscht werden. Wenn Sie eine gerade verwendete Snapshot-Definition löschen, wird der Export der Daten in die Snapshot-Datenbank gestoppt. Die Snapshot-Definition ist aber weiterhin verfügbar.

Snapshot-Daten erfassen

Wenn Sie Snapshot-Daten sofort erfassen oder Snapshot-Daten später bzw. regelmäßig exportieren möchten, führen Sie die Aufgabe "Snapshot-Daten erfassen" aus. Diese Aufgabe exportiert die Daten sofort (durch die Snapshot-Definition definiert) in die Snapshot-Datenbank.

Wichtig! Der Export von Snapshot-Daten kann viel Zeit in Anspruch nehmen, wenn große Datenmengen zu exportieren sind. Es ist zu empfehlen, die Snapshots zu planen, wenn große Datenmengen exportiert werden.

So erfassen Sie Snapshot-Daten:

1. Navigieren Sie in der Benutzerkonsole zu "Berichte", "Snapshot-Aufgaben", "Snapshot-Daten erfassen".
2. Wählen Sie "Jetzt ausführen" aus, um die Daten sofort zu exportieren, oder wählen Sie Neuen Job planen (siehe Seite 443) aus, um den Datenexport zu einem späteren Zeitpunkt oder nach einem Zeitplan auszuführen.
3. Klicken Sie auf "Weiter".
4. Wählen Sie eine Snapshot-Definition aus.
5. Klicken Sie auf "Senden".

   Die Snapshot-Daten werden in die Snapshot-Datenbank exportiert.

Hinweis: Falls die Aufgabe "Snapshot-Daten erfassen" sehr viel Zeit in Anspruch nimmt, können Sie den Fortschritt der Aufgabe prüfen, indem Sie zur Registerkarte "System" wechseln und auf "Gesendete Aufgaben anzeigen" klicken.

Registerkarte "Wiederholungen"

Planen Sie Ihren Job auf dieser Registerkarte. Diese Registerkarte enthält die folgenden Felder:

Jetzt ausführen

Führt den Job sofort aus.

Neuen Job planen

Plant einen neuen Job.

Vorhandenen Job ändern

Gibt an, dass Sie einen bereits vorhandenen Job ändern möchten.

Hinweis: Dieses Feld wird nur angezeigt, wenn ein Job bereits für diese Aufgabe geplant wurde.

Jobname

Gibt den Namen des Jobs an, den Sie erstellen oder ändern möchten.

Zeitzone

Gibt die Serverzeitzone an.

Hinweis: Wenn Ihre Zeitzone sich von der Zeitzone des Servers unterscheidet, wird beim Planen eines neuen Jobs eine Dropdown-Liste angezeigt, damit Sie entweder Ihre Zeitzone oder die Zeitzone Ihres Servers auswählen können. Sie können die Zeitzone beim Ändern eines vorhandenen Jobs nicht anpassen.

Täglicher Ablaufplan

Gibt an, dass der Job immer nach einer bestimmten Anzahl von Tagen ausgeführt wird.

Alle (Anzahl der Tage)

Definiert, wie viele Tage zwischen den Jobausführungen liegen.

Wöchentlicher Ablaufplan

Gibt an, dass der Job an einem bestimmten Tag bzw. bestimmten Tagen und zu einem bestimmten Zeitpunkt in der Woche ausgeführt wird.

Wochentag

Legt den Tag bzw. die Tage in der Woche fest, an dem bzw. denen der Job ausgeführt wird.

Monatlicher Ablaufplan

Legt einen Tag der Woche oder des Monats fest, an dem der Job monatlich ausgeführt wird.

Jährlicher Ablaufplan

Legt einen Tag der Woche oder des Monats fest, an dem der Job jährlich ausgeführt wird.

Erweiterter Ablaufplan

Legt zusätzliche Zeitplaninformationen fest.

Cron-Ausdruck

Informationen zum Ausfüllen dieses Feldes finden Sie unter

http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html

Ausführungszeit

Gibt die Tageszeit zum Ausführen des Jobs im 24-Stunden-Format an. Beispiel: 14:15.

Einer Berichtsaufgabe eine Snapshot-Definition zuweisen

Weisen Sie einer Berichtsaufgabe eine Snapshot-Definition zu, damit CA IdentityMinder weiß, welche Snapshot-Definition bei der Ausführung des Berichts verwendet werden soll. Informationen für CA IdentityMinder-Berichte können aus unterschiedlichen Quellen stammen. Jeder Bericht muss einer spezifischen Datenquelle zugeordnet werden, je nachdem, welche Informationen der Bericht enthalten soll.

So weisen Sie einer Berichtsaufgabe eine Snapshot-Definition und eine Verbindung zu

1. Wählen Sie in der Benutzerkonsole die Optionen "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe ändern" aus.
2. Suchen Sie nach der Berichtsaufgabe, der Sie eine Snapshot-Definition zuweisen möchten.
3. Wechseln Sie zur Registerkarte "Registerkarten" und klicken Sie neben der Registerkarte "Snapshot-Definitionen zuordnen" auf .
4. Klicken Sie auf "Hinzufügen".
5. Suchen Sie nach der Berichtsaufgabe, der eine Snapshot-Definition zugewiesen werden soll, und klicken Sie auf "Auswählen".

   Bei der Zuweisung einer Snapshot-Definition zu einer Berichtsaufgabe sollten Sie folgendes beachten:

   - Einem Bericht können mehrere Snapshot-Definitionen zugewiesen werden.
   - Eine Snapshot-Definition kann mehreren Berichten zugewiesen werden.
   - Sind einer einzelnen Berichtsaufgabe mehrere Snapshots zugewiesen, müssen diese nicht dieselbe Wiederholungszeit verwenden.
6. Klicken Sie auf "OK".
7. Wechseln Sie zur Registerkarte "Suchen" und klicken Sie auf "Durchsuchen", um die Suchfenster zu öffnen.
8. Bearbeiten Sie das Suchfenster für die Berichtsaufgabe, und wählen Sie unter "Verbindungsobjekt für den Bericht" die Option "rptParamConn" aus.
9. Klicken Sie auf "OK".
10. Klicken Sie auf "Auswählen".
11. Klicken Sie auf "Senden".

Bericht anfordern

Um den Bericht anzuzeigen, fordern Sie einen Bericht bei einem Benutzer mit Berechtigungen zur Berichtsverwaltung an. Eine Genehmigung ist erforderlich, weil einige Berichte eine lange Zeit oder bedeutende Systemressourcen zur Ausführung benötigen können. Wenn Ihre Berichtsanfrage eine Genehmigung benötigt, sendet Ihnen das System eine E-Mail-Warnmeldung.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole mit Benutzerberechtigungen für Berichtsaufgaben an.
2. Wählen Sie "Berichte", "Berichtsaufgaben", "Bericht anfordern".

   Eine Liste der Berichte wird angezeigt.
3. Wählen Sie den Bericht aus, der angefordert werden soll.

   Ein Parameterfenster wird angezeigt.

   Geben Sie die erforderlichen Parameterdaten ein.

   Hinweis: Wenn Sie einen Snapshot-Bericht ausführen und keine Snapshots für diesen Bericht vorhanden sind, müssen Sie zunächst einen Snapshot aufzeichnen.

   - Einige Berichte zeigen den Systemzustand an einem bestimmten Zeitpunkt. Wenn Sie diesen Typ Bericht anfordern, wählen Sie einen Zeitpunkt aus, für den Sie Berichtsdaten sehen möchten. Dieser Zeitpunkt wird *Snapshot* genannt.

     Hinweis: Die Snapshot-Daten und -Zeiten, die Sie wählen können, sind vorbestimmt. Normalerweise führt der Systemadministrator oder ein anderer Benutzer mit Berichtsverwaltungsrechten diese Snapshot-Konfiguration aus. Wenn keine Snapshots für den Bericht verfügbar sind, den Sie anfordern möchten, setzen Sie sich mit einem Systemadministrator in Verbindung.
   - Einige Berichte zeigen die Aktivität über einen Zeitraum. Die Titel für diese Berichte fangen üblicherweise mit dem Wort *Audit* an. Wenn Sie diesen Typ Bericht anfordern, wählen Sie einen Zeitraum aus, für den Sie Berichtsdaten sehen möchten. Zum Beispiel können Sie den Audit-Bericht über Kennwortzurücksetzungen für die letzten 30 Tage ausführen.

4. Klicken Sie auf "Bericht planen", und wählen Sie einen Ablaufplan für Ihren Bericht aus.

   Jetzt

   Gibt an, dass der Bericht sofort ausgeführt wird.

   Einmal

   Gibt an, dass der Bericht einmal während eines bestimmten Zeitraums ausgeführt wird. Wählen Sie zum Generieren des Berichts die Start- und Endzeit sowie das Start- und Enddatum aus.

   Hinweis: Ziehen Sie diese Option in Betracht, wenn der Bericht, den Sie anfordern, eine große Datenmenge benötigt. Um Systemressourcen zu sparen, sollten Sie eine Zeit mit geringer Systemaktivität wählen.

5. Klicken Sie auf "Senden".

   Die Berichtsanfrage wird gesendet. Je nach Umgebungskonfiguration wird die Anfrage sofort oder nach Genehmigung von einem Administrator ausgeführt.

   Normalerweise müssen ein Systemadministrator oder ein anderer Benutzer mit Berichtsverwaltungsberechtigungen eine Berichtsanfrage genehmigen, bevor das System sie fertig stellt. Eine Genehmigung ist erforderlich, weil einige Berichte eine lange Zeit oder bedeutende Systemressourcen benötigen können. Wenn Ihre Berichtsanfrage eine Genehmigung benötigt, sendet Ihnen das System eine E-Mail-Warnung.

Anzeigen des Berichts

Je nach Umgebungskonfiguration wird ein Bericht zur Anzeige verfügbar, wenn ein Administrator die Anfrage für diesen Bericht genehmigt hat. Wenn Ihre Berichtsanfrage eine Genehmigung benötigt, sendet Ihnen das System eine E-Mail-Warnung. Der Bericht, den Sie anzeigen möchten, wird in der Suchliste nicht angezeigt, bis er genehmigt wird.

Hinweis: Damit Sie unter Verwendung der Aufgabe "Meine Berichte anzeigen" in CA IdentityMinder Berichte anzeigen können, müssen Sie in Ihrem Browser Sitzungscookies von Drittanbietern zulassen.

Gehen Sie wie folgt vor:

1. Wechseln Sie in der Benutzerkonsole zu "Berichte", "Berichtsaufgaben", und klicken Sie auf "Meine Berichte anzeigen".
2. Suchen Sie den generierten Bericht, den Sie anzeigen möchten.

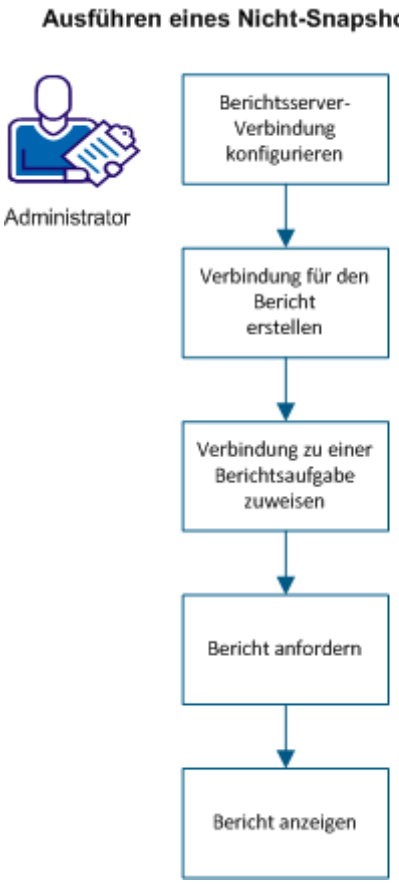
   Es werden sowohl Wiederholungsberichte als auch Instanzen von Berichten bei Bedarf angezeigt.

   Hinweis: Wenn der Status des Berichts "Ausstehend/Wiederholend" lautet, wird der Bericht nicht generiert und es kann länger dauern, den Bericht abzuschließen.
3. Wählen Sie den Bericht aus, der angezeigt werden soll.
4. (Optional) Klicken Sie oben links auf "Diesen Bericht exportieren", um den Bericht in den folgenden Formaten zu exportieren:
   - Crystal Reports
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) - nur Daten
   - Microsoft Excel (97-2003) - Bearbeitbar
   - Rich Text Format (RTF)
   - Getrennte Werte (CSV)
   - XML

So führen Sie einen Nicht-Snapshot-Bericht aus

Ein Nicht-Snapshot-Bericht enthält Daten aus anderen Datenquellen, wie z. B. aus Audit-, Workflow- oder Aufgabenpersistenz-Datenbanken. CA IdentityMinder enthält in der Benutzerkonsole standardmäßige Audit-Berichte mit dem Präfix "Audit-" im Namen. Standardmäßig enthält CA IdentityMinder nur Audit-Berichte, aber Sie können Ihre eigenen benutzerdefinierten Berichte erstellen, die Daten von einer beliebigen Datenquelle enthalten können.

Dieses Szenario beschreibt, wie ein Super-Administrator eine Berichtsdatenbankverbindung konfiguriert und einen Nicht-Snapshot-Bericht ausführt.



Folgendes Diagramm veranschaulicht den Prozess für die Ausführung eines Snapshot-Berichts:

Um den Nicht-Snapshot-Bericht auszuführen, führen Sie folgende Schritte aus:

1. Konfigurieren Sie die Berichtsserver-Verbindung. (siehe Seite 450)
2. Erstellen Sie eine Verbindung für den Bericht. (siehe Seite 451)
3. Weisen Sie der Berichtsaufgabe eine Verbindung zu. (siehe Seite 451)

4. Fordern Sie einen Bericht an. (siehe Seite 446)
5. Zeigen Sie den Bericht an. (siehe Seite 448)

Berichtsserver-Verbindung konfigurieren

Um Daten vom Berichtsserver zu erfassen, müssen Sie die Verbindung zum Berichtsserver konfigurieren. Bevor Sie mit dem Vorgang beginnen, sammeln Sie folgende Informationen über den Berichtsserver:

Name	Beschreibung
Hostname	Der Hostname des Rechners, auf dem der Berichtsserver installiert ist
Port	Der Portname des Rechners, auf dem der Berichtsserver installiert ist
Berichtsordnername	Der Speicherort der standardmäßigen CA IdentityMinder-Berichte.
Benutzer-ID	Gibt den Benutzer an, der für den Berichtsserver erstellt wurde.
Kennwort	Gibt das Kennwort für den Benutzer an, der im Berichtsserver erstellt wurde.
Sichere Verbindung	Gibt die Sicherheitsverbindung für den Berichtsserver an. Aktivieren Sie das Kontrollkästchen, um eine SSL-Verbindung (Secure Sockets Layer) zwischen CA IdentityMinder und dem Berichtsserver zu ermöglichen. **Hinweis**: Bevor Sie das Kontrollkästchen "Sichere Verbindung" aktivieren, überprüfen Sie, dass Sie das Zertifikat vom BOServer installiert haben. Weitere Informationen darüber, wie Sie SSL richtig konfigurieren, finden Sie im Kapitel "Berichtsserver-Installation" im *Installationshandbuch*.
Webserver	Gibt den Webserver an. Für Tomcat auf Nicht-IIS gesetzt.

Hinweis: Wir empfehlen, dass für alle Systeme, die an der Berichterstellung beteiligt sind, dieselbe Zeitzone und Uhrzeit festgelegt wird.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Benutzerkonsole auf "System", "Berichterstellung", "Berichtsserver-Verbindung".
2. Geben Sie die Einstellungen für den Berichtsserver ein.
3. Klicken Sie auf "Verbindung testen", um die Verbindung zu überprüfen.
4. Klicken Sie auf "Senden".

Die Berichtsverbindung ist hergestellt.

Erstellen einer Verbindung für den Bericht

Informationen für CA IdentityMinder-Berichte können aus unterschiedlichen Quellen stammen. Erstellen Sie eine JDBC-Verbindung in CA IdentityMinder, um Details zu einer Verbindung mit einer zusätzlichen Datenquelle für den Bericht anzugeben.

Gehen Sie wie folgt vor:

1. Navigieren Sie in der Benutzerkonsole zu "System", "JDBC-Verbindungsverwaltung", "JDBC-Verbindung herstellen".
2. Erstellen Sie ein neues Verbindungsobjekt, oder wählen Sie ein Verbindungsobjekt basierend auf einer spezifischen JNDI-Datenquelle aus.
3. Füllen Sie alle erforderlichen Felder aus, und klicken Sie auf "Senden".

   Es wird eine neue JDBC-Verbindung erstellt.

Wichtig! Es wird empfohlen, dass Sie *nicht* die CA IdentityMinder-Objektspeicher-Datenbank zum Generieren von Berichten verwenden.

Zuweisen einer Verbindung zu einer Berichtsaufgabe

Informationen für CA IdentityMinder-Berichte werden aus unterschiedlichen Quellen erfasst. Jeder Bericht muss einer spezifischen Datenquelle zugeordnet werden, je nachdem, welche Informationen der Bericht enthalten soll.

So weisen Sie einer Berichtsaufgabe eine Verbindung zu:

1. Wählen Sie in der Benutzerkonsole die Optionen "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe ändern" aus.
2. Suchen Sie nach der Berichtsaufgabe, der Sie eine Verbindung zuweisen möchten.
3. Wechseln Sie zur Registerkarte "Suchen" und klicken Sie auf "Durchsuchen", um die Suchfenster zu öffnen.
4. Bearbeiten Sie das Suchfenster für die Berichtsaufgabe, und wählen Sie unter "Verbindungsobjekt für den Bericht" eine Verbindung aus.
5. Klicken Sie auf "OK".
6. Klicken Sie auf Auswählen.
7. Klicken Sie auf "Senden".

Bericht anfordern

Um den Bericht anzuzeigen, fordern Sie einen Bericht bei einem Benutzer mit Berechtigungen zur Berichtsverwaltung an. Eine Genehmigung ist erforderlich, weil einige Berichte eine lange Zeit oder bedeutende Systemressourcen zur Ausführung benötigen können. Wenn Ihre Berichtsanfrage eine Genehmigung benötigt, sendet Ihnen das System eine E-Mail-Warnmeldung.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole mit Benutzerberechtigungen für Berichtsaufgaben an.
2. Wählen Sie "Berichte", "Berichtsaufgaben", "Bericht anfordern".

   Eine Liste der Berichte wird angezeigt.
3. Wählen Sie den Bericht aus, der angefordert werden soll.

   Ein Parameterfenster wird angezeigt.

   Geben Sie die erforderlichen Parameterdaten ein.

   Hinweis: Wenn Sie einen Snapshot-Bericht ausführen und keine Snapshots für diesen Bericht vorhanden sind, müssen Sie zunächst einen Snapshot aufzeichnen.

   - Einige Berichte zeigen den Systemzustand an einem bestimmten Zeitpunkt. Wenn Sie diesen Typ Bericht anfordern, wählen Sie einen Zeitpunkt aus, für den Sie Berichtsdaten sehen möchten. Dieser Zeitpunkt wird *Snapshot* genannt.

     Hinweis: Die Snapshot-Daten und -Zeiten, die Sie wählen können, sind vorbestimmt. Normalerweise führt der Systemadministrator oder ein anderer Benutzer mit Berichtsverwaltungsrechten diese Snapshot-Konfiguration aus. Wenn keine Snapshots für den Bericht verfügbar sind, den Sie anfordern möchten, setzen Sie sich mit einem Systemadministrator in Verbindung.
   - Einige Berichte zeigen die Aktivität über einen Zeitraum. Die Titel für diese Berichte fangen üblicherweise mit dem Wort *Audit* an. Wenn Sie diesen Typ Bericht anfordern, wählen Sie einen Zeitraum aus, für den Sie Berichtsdaten sehen möchten. Zum Beispiel können Sie den Audit-Bericht über Kennwortzurücksetzungen für die letzten 30 Tage ausführen.

4. Klicken Sie auf "Bericht planen", und wählen Sie einen Ablaufplan für Ihren Bericht aus.

   Jetzt

   Gibt an, dass der Bericht sofort ausgeführt wird.

   Einmal

   Gibt an, dass der Bericht einmal während eines bestimmten Zeitraums ausgeführt wird. Wählen Sie zum Generieren des Berichts die Start- und Endzeit sowie das Start- und Enddatum aus.

   Hinweis: Ziehen Sie diese Option in Betracht, wenn der Bericht, den Sie anfordern, eine große Datenmenge benötigt. Um Systemressourcen zu sparen, sollten Sie eine Zeit mit geringer Systemaktivität wählen.

5. Klicken Sie auf "Senden".

   Die Berichtsanfrage wird gesendet. Je nach Umgebungskonfiguration wird die Anfrage sofort oder nach Genehmigung von einem Administrator ausgeführt.

   Normalerweise müssen ein Systemadministrator oder ein anderer Benutzer mit Berichtsverwaltungsberechtigungen eine Berichtsanfrage genehmigen, bevor das System sie fertig stellt. Eine Genehmigung ist erforderlich, weil einige Berichte eine lange Zeit oder bedeutende Systemressourcen benötigen können. Wenn Ihre Berichtsanfrage eine Genehmigung benötigt, sendet Ihnen das System eine E-Mail-Warnung.

Anzeigen des Berichts

Je nach Umgebungskonfiguration wird ein Bericht zur Anzeige verfügbar, wenn ein Administrator die Anfrage für diesen Bericht genehmigt hat. Wenn Ihre Berichtsanfrage eine Genehmigung benötigt, sendet Ihnen das System eine E-Mail-Warnung. Der Bericht, den Sie anzeigen möchten, wird in der Suchliste nicht angezeigt, bis er genehmigt wird.

Hinweis: Damit Sie unter Verwendung der Aufgabe "Meine Berichte anzeigen" in CA IdentityMinder Berichte anzeigen können, müssen Sie in Ihrem Browser Sitzungscookies von Drittanbietern zulassen.

Gehen Sie wie folgt vor:

1. Wechseln Sie in der Benutzerkonsole zu "Berichte", "Berichtsaufgaben", und klicken Sie auf "Meine Berichte anzeigen".
2. Suchen Sie den generierten Bericht, den Sie anzeigen möchten.

   Es werden sowohl Wiederholungsberichte als auch Instanzen von Berichten bei Bedarf angezeigt.

   Hinweis: Wenn der Status des Berichts "Ausstehend/Wiederholend" lautet, wird der Bericht nicht generiert und es kann länger dauern, den Bericht abzuschließen.
3. Wählen Sie den Bericht aus, der angezeigt werden soll.
4. (Optional) Klicken Sie oben links auf "Diesen Bericht exportieren", um den Bericht in den folgenden Formaten zu exportieren:
   - Crystal Reports
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) - nur Daten
   - Microsoft Excel (97-2003) - Bearbeitbar
   - Rich Text Format (RTF)
   - Getrennte Werte (CSV)
   - XML

Festlegen von Berichtsoptionen

Konfigurieren Sie die Anzahl der Berichtsinstanzen, die ein Benutzer für einen bestimmten Bericht generieren kann.

So ändern Sie die Berichtsoptionen:

1. Wählen Sie "Berichte", "Berichtsaufgaben" und dann "Berichtsoptionen festlegen".

   CA IdentityMinder stellt eine Verbindung mit dem IAM-Berichtsserver her und ruft eine Liste aller Berichte ab.

2. Wählen Sie einen Bericht aus, und klicken Sie auf "Ändern".

   Das Attributfenster des Berichts wird angezeigt.

3. Bearbeiten Sie die folgenden Felder:

   Name

   Gibt den Anzeigenamen des ausgewählten Berichts an.

   Anzahl der Instanzen

   Gibt die zulässige Anzahl von Instanzen dieses Berichts an, die ein Benutzer generieren darf.

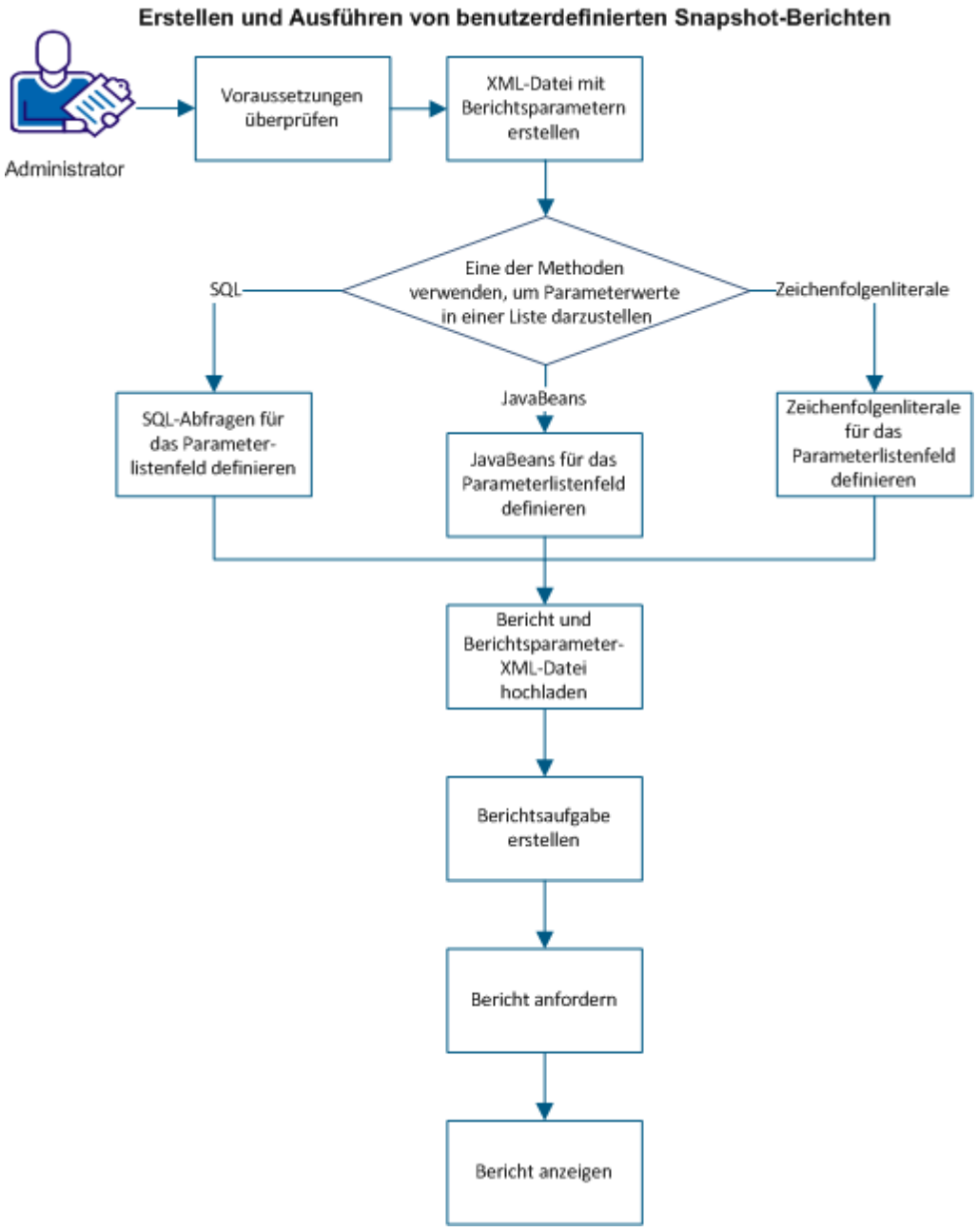
4. Klicken Sie auf "OK".

   Die Berichtsattribute werden geändert.

So können Sie einen benutzerdefinierten Snapshot-Bericht erstellen und ausführen

In CA IdentityMinder können Sie Berichte erstellen und Ihren Geschäftsanforderungen gemäß anpassen. CA IdentityMinder stellt eine XML-Datei mit Berichtsparametern bereit, die alle Parameter enthält, die sich auf Berichterstellungsattribute beziehen. Entsprechend Ihren Geschäftsanforderungen können Sie die erforderlichen Attribute auswählen, um Berichtsdaten von der Snapshot-Datenquelle aufzufüllen.

Folgende Grafik veranschaulicht den Prozess, um einen benutzerdefinierten Snapshot-Bericht zu erstellen und auszuführen:



Stellen Sie als Systemadministrator folgende Schritte fertig:

1. Überprüfen der Voraussetzungen (siehe Seite 458)
2. Erstellen der XML-Datei mit den Berichtsparametern (siehe Seite 458)
3. Verwenden Sie eine der folgenden Methoden, um Parameterwerte für eine Liste darzustellen:
   - Definieren Sie SQL-Abfragen für das Listenfeld "Parameter" (siehe Seite 462)

- Definieren Sie Java-Beans für das Listenfeld "Parameter" (siehe Seite 463)
- Definieren Sie Zeichenfolgenliterale für das Listenfeld "Parameter" (siehe Seite 463)

4. Hochladen des Berichts und der XML-Datei mit den Berichtsparametern (siehe Seite 463)
5. Erstellen Sie die Berichtsaufgabe (siehe Seite 465)
6. Fordern Sie einen Bericht an (siehe Seite 468)
7. Zeigen Sie einen Bericht an (siehe Seite 448)

Erstellen von Berichten in Crystal Reports Developer

Damit Sie benutzerdefinierte Berichte in CA IdentityMinder verwenden können, erstellen Sie einen Bericht (RPT-Datei) in Crystal Reports Developer. Weitere Informationen zum Erstellen von Berichten in Crystal Reports finden Sie in der Dokumentation zu Crystal Reports.

Hinweis: Das CA IdentityMinder-Datenbankschema befindet sich im folgenden Speicherort (falls Sie auf das CA IdentityMinder-Schema verweisen müssen, um benutzerdefinierte Berichte zu erstellen):

```
<Installationspfad>\db\objectstore
```

Erstellen der XML-Datei mit den Berichtsparametern

Bei einem Parameter handelt es sich um eins der Felder in einem Bericht, die zum Filtern der Berichte verwendet werden können. Sie können einen Bericht generieren, indem Sie die Daten mithilfe von Parametern filtern. Um eine benutzerspezifische Anpassung des Berichtssuchfensters zu ermöglichen, wird jeder Bericht (RPT-Datei) einer XML-Datei mit Berichtsparametern zugeordnet. In CA IdentityMinder können Sie Berichtsaufgaben und Suchfenster erstellen, sodass ein Benutzer während der Generierung eines Berichts erforderliche Daten eingeben oder auswählen kann.

Hinweis: Eine XML-Datei mit Berichtsparametern ist nur erforderlich, wenn der Bericht Attribute des Objekts abfragt.

Die XML-Datei mit den Berichtsparametern muss denselben Namen wie der Bericht (RPT-Datei) mit der Erweiterung ".xml" haben. Wenn Sie zum Beispiel einen Bericht mit dem Namen "test1.rpt" in den Berichtsserver hochladen, sollte die XML-Datei "test1.xml" genannt werden.

Die XML-Datei mit den Berichtsparametern enthält folgende Elemente:

<product>

Identifiziert das Produkt, für das die Parameter verwendet werden. Sie können unterschiedliche Parameter für mehrere Produkte mithilfe der gleichen Parameter-XML-Datei erstellen.

<screen>

Definiert die Parameter, die in einem Fenster anzeigt werden. Sie können das Fensterelement verwenden, um die Parameter an ein bestimmtes Fenster zu binden. Die Fenster-ID ist alphanumerisch und eindeutig. Sie wird verwendet, um die Fenster und ihre Parameter zu identifizieren.

<parameters>

Gibt die Sammlung von Parametern für ein Fenster an.

<param>

Definiert das Parameterelement, das angegebene Daten an den Bericht weitergibt. Die folgenden Attribute werden im <param>-Element verwendet:

id

Legt fest, mit welchem Parameter im Bericht eine Zuordnung erstellt werden soll.

Hinweis: Die ID muss denselben Namen wie der Parameter im Crystal Report haben.

name

Dieses Feld wird in CA IdentityMinder gegenwärtig nicht verwendet. Legen Sie dieses Attribut auf den gleichen Wert wie für "id" fest.

displaytext

Gibt den benutzerfreundlichen Text an, der im Fenster für den Parameter angezeigt werden soll.

type

Gibt den Typ des Parameters an. Die Fensteranzeige ändert sich basierend auf diesem Attribut. Die folgenden Parametertypen werden unterstützt:

- **Textfeld**

  Beispiel: <param id="param1" displaytext="First Name" name="param1" type="string"/>

- **Datum und Uhrzeit**

  Beispiel: <param id="dateVal" displaytext="Date" name="dateVal" type="date_str"/>

  <param id="timeVal" displaytext="Time" name="timeVal" type="time_str"/>

  <param id="datetimeVal" displaytext="Date & Time" name="datetimeVal" type="date_time_str"/>

- **Drop-down-Liste**

  Beispiel: <param id="lastname1" displaytext="Name" name="lastname1" type="dropdown" default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>

- **Listenfeld**

  Beispiel: <param id="lstlastname1" displaytext="Name" name="lstlastname1" type="listbox" rows="10" default="key1%1FSuper%1Ekey2%1Fsql2kSuser01%1E key1F%Super"/>

- **Optionsfeld**

  Beispiel: <param id="optionslist" displaytext="Option 1" name="optionslist" type="radiobox" value="option1"/>

  <param id="optionslist" displaytext="Option 2" name="optionslist" type="radiobox" value="option2"/>

  <param id="optionslist" displaytext="Option 3" name="optionslist" type="radiobox" value="option3"/>

- **Kontrollkästchen**

  Beispiel: <param id="enabled" displaytext="Enabled" name="enabled" type="checkbox"/>

row

Legt fest, wie viele Zeilen in einem Listenfeld sichtbar sind.

Standard: 5

default

Legt den Standardwert fest, der im Fenster für einen bestimmten Parameter angezeigt wird. Dieses Attribut kann mit folgenden Typen verwendet werden: Zeichenfolge, Listenfeld und Drop-down-Liste.

Definieren Sie SQL-Abfragen für das Listenfeld "Parameter"

Sie können SQL-Abfragen als Teil eines Listenfelds oder Drop-down-Felds in der XML-Datei mit den Berichtsparametern definieren. Wenn Sie einen Parameter zum Bericht zuordnen und eine Berichtsaufgabe erstellen, dann wird der Parameter im Listenfeld oder im Drop-down-Feld angezeigt. Um SQL im Drop-down-Feld oder Listenfeldparameter zu verwenden, geben Sie eine gültige SQL-Anweisung im SQL-Attribut an.

Beispiel:

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname like
'S%/>
```

Im vorherigen Beispiel werden alle Nachnamen von Benutzern, deren Vorname mit "*S*" anfängt, für den Bericht abgerufen.

Die Bedingung, dass der Vorname mit "*S*" anfängt, ist jedoch statisch. Diese Abfrage ist nicht flexibel genug, damit ein Benutzer den Wert basierend auf dem Parameterwert laden kann, der in einem der vorherigen Fenster eingegeben und in der gleichen Berichtsparametergruppe verwendet wurde. Um einen Wert zu verwenden, der zuvor in einem anderen Fenster eingegeben wurde, kann die SQL-Anweisung mit "*##<parameter id>##*" erweitert werden.

Wenn Sie beispielsweise einen Parameter mit "id=User" und "type=string" haben:

```
<param id="User" displaytext="First Name" name="firstname" type="string"/>
```

Wenn Sie den Eingabewert für diesen Parameter in SQL verwenden möchten, kann die SQL-Anweisung folgendermaßen lauten:

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname like
'##User##'/>
```

CA IdentityMinder ersetzt ##User## mit dem Wert, der für den Parameter mit "id=User" eingegeben wurde.

Hinweis: Der zu ersetzende Parameterwert darf sich nicht im gleichen Fenster wie der SQL-Parameter befinden. Wenn zum Beispiel "*lstlastname2*" im Fenster 3 vorkommt, sollte sich der Benutzerparameter in einem der vorherigen Fenster befinden.

Definieren Sie Java-Beans für das Listenfeld "Parameter"

Wenn SQL nicht geeignet ist, können Sie Java Beans verwenden, um Werte zu berechnen und die Liste der <Schlüssel, Wert>-Paare an CA IdentityMinder zu übergeben. Die JavaBeans sollten sich im Klassenpfad von CA IdentityMinder befinden.

Beispiel:

```
<param id="lastname2" displaytext="Name using Javabean" name="lastname2"
type="dropdown" class="com.ca.ims.reporting.unittests.TestDataCollector"/>
```

Im vorherigen Beispiel ruft TestDataCollector die Werte mit der eigenen Methode ab und übergibt die Daten für die Drop-down-Liste an den Bericht. Die <Schlüssel, Wert>-Paare sind durch %1F getrennt.

Vergewissern Sie sich, dass sich die JavaBean im Verzeichnis "iam_im.ear\custom" befindet.

Hinweis: Weitere Informationen zum Implementieren von JavaBeans finden Sie in der BusinessObjects-Dokumentation.

Definieren Sie Zeichenfolgenliterale für das Listenfeld "Parameter"

Die einfachste Methode, um die Parameterwerte für ein Listen- oder Drop-down-Feld darzustellen, besteht in der Verwendung von Zeichenfolgenliteralen. Der Schlüsselwert wird durch %1F getrennt, und jedes <Schlüssel, Wert>-Paar wird durch %1E getrennt.

Beispiel:

```
<param id="lastname1" displaytext="Name" name="lastname" type="dropdown"
default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>
```

Hochladen des Berichts und der XML-Datei mit den Berichtsparametern

Nachdem Sie den Bericht (RPT) und die entsprechende XML-Datei mit den Berichtsparametern erstellt haben, laden Sie beide Dateien auf den Berichtsserver hoch (BusinessObjects).

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der zentralen Management-Konsole von BusinessObjects an.
2. Klicken Sie auf "Ordner".
3. Wählen Sie den Ordner "IM Reports" (IM-Berichte) aus.
4. Erstellen Sie ein Objektpaket.
5. Navigieren Sie durch das neue Objektpaket, um den Crystal Report hinzuzufügen.

6. Suchen Sie nach dem neuen Bericht (RPT), den Sie erstellt haben.

   Hinweis: Stellen Sie sicher, dass der Ordner "IM Reports" (IM-Berichte) als Ordner ausgewählt ist, in dem der Bericht gespeichert wird.

7. Klicken Sie auf "OK".

   Die Crystal Report-Datei ist hinzugefügt.

8. Fügen Sie im neuen Objektpaket ein neues lokales Dokument hinzu, und navigieren Sie zur neuen XML-Datei mit Berichtsparametern.

9. Wählen Sie den Dateityp "*Text*" aus.

10. Klicken Sie auf "OK".

Der Bericht und die XML-Datei mit Berichtsparametern sind jetzt hochgeladen. Um dies zu überprüfen, gehen Sie zum IM-Berichtsordner, und überprüfen Sie, ob beide neue Dateien verfügbar sind.

Erstellen der Berichtsaufgabe

Berichtsaufgaben werden verwendet, um die Vorlagen für die in der Benutzerkonsole generierten Berichte zu erstellen, zu verwalten, anzuzeigen und zu löschen.

Gehen Sie wie folgt vor:

1. Wählen Sie in der Benutzerkonsole die Optionen "Rollen und Aufgaben", "Admin-Aufgabe", "Admin-Aufgabe erstellen" aus.
2. Wählen Sie "Neue Admin-Aufgabe erstellen" aus, und klicken Sie auf "OK".
3. Füllen Sie die folgenden Felder auf der Registerkarte "Profil" aus:

   Name

   Gibt den Namen des Berichts an. Jeder Berichtsaufgabenname sollte eindeutig sein.

   Tag

   Gibt den eindeutigen Bezeichner für die Aufgabe an. Diese Angabe wird in einer URL, einem Webservice oder einer Eigenschaftsdatei verwendet. Sie muss aus Buchstaben, Zahlen und/oder Unterstrichen bestehen und mit einem Buchstaben oder Unterstrich beginnen.

   Kategorie

   Gibt die Kategorie an, zu der die aktuelle Aufgabe gehört.

   Hinweis: Wählen Sie die Kategorie "Berichte" aus.

   Kategorie 2

   Gibt die Unterkategorie an, zu der die aktuelle Aufgabe gehört. Geben Sie eine beliebige Zeichenfolge in dieses Feld ein.

   Primäres Objekt

   Gibt das Objekt an, für das die Aufgabe angewendet wird.

   Hinweis: Wählen Sie "Berichtinstanz" als primäres Objekt aus.

   Aktion

   Gibt die Aktion an, die für das primäre Objekt ausgeführt wird.

   Hinweis: Wählen Sie "Erstellen" als Aktion aus.
4. Um ein neues Suchfenster für die Berichtsaufgabe zu erstellen, führen Sie folgende Schritte aus:
   a. Klicken Sie auf der Registerkarte "Suchen" auf "Durchsuchen", um die Suchfenster zu öffnen.

      Die Liste der verfügbaren Suchfenster wird angezeigt.

   b. Klicken Sie auf "Neu".

      Das Fenster "Fenster erstellen" wird angezeigt.

c. Wählen Sie "Berichtsvorlage - Auswahlfenster" aus der Liste aus, und klicken Sie auf "OK".

   CA IdentityMinder stellt eine Verbindung mit dem Berichtsserver her und zeigt alle Berichte an.

d. Füllen Sie die folgenden Felder aus:

   Name

   Gibt den Namen des Berichts an. Jeder Berichtsaufgabenname sollte eindeutig sein.

   Tag

   Agiert als eindeutige Kennung innerhalb einer Aufgabe. Sie darf Buchstaben (a-z, A-Z), Zahlen (0-9) oder Unterstriche enthalten und muss mit einem Zeichen oder Unterstrich beginnen.

   Titel

   Definiert den Titel des neuen Suchfensters. Der Titel muss eindeutig sein.

   Berichtsvorlage

   Identifiziert den Bericht, der dem Suchfenster zugeordnet werden soll.

   Hinweis: Wählen Sie einen der Berichte aus, den Sie dem Berichtsserver hinzugefügt haben.

   Verbindungsobjekt für den Bericht

   Definiert die Verbindungsdetails der Datenquelle, die für den Bericht verwendet werden soll.

5. Klicken Sie auf "OK".

   Das neue Suchfenster wird jetzt für Berichte erstellt.

6. Führen Sie auf der Registerkarte zur Erstellung einer Registerkarte für die Berichtsaufgabe folgende Schritte aus:

   a. Klicken Sie auf "Registerkarten".

      Die Registerkarten, die für den Benutzer sichtbar sind, werden angezeigt.

   b. Wählen Sie "Standard-Registerkartensteuerung" aus.

   c. Wenn Ihr Bericht eine Snapshot-Definition verwendet, führen Sie folgende Schritte aus:

      a. Wählen Sie unter "Welche Registerkarten sollen in dieser Aufgabe angezeigt werden?" die Option "Snapshot-Definitionen zuordnen" aus.

         Die Registerkarte "Snapshot-Definitionen zuordnen" wird zu der Liste der Registerkarten hinzugefügt.

      b. Klicken Sie auf , um die Registerkarte "Snapshot-Definitionen zuordnen" zu bearbeiten.

Das Konfigurationsfenster "Snapshot-Definitionen zuordnen" wird angezeigt.

c. Klicken Sie auf "Hinzufügen", um die Berichtsaufgabe einer Snapshot-Definition zuzuordnen.

   Eine Liste der verfügbaren Snapshot-Definitionen wird angezeigt.

d. Wählen Sie eine Snapshot-Definition aus, und klicken Sie auf "OK".

   Die Berichtsaufgabe wird einer Snapshot-Definition zugeordnet.

d. Klicken Sie auf "Senden".

   Die Berichtsaufgabe wird erstellt.

e. Weisen Sie die neue Berichtsaufgabe einer Admin-Rolle zu.

   Die CA IdentityMinder-Admin-Rollenbenutzer können die neue Berichtsaufgabe verwenden.

Die Berichtsaufgabe kann jetzt vom Admin verwendet werden.

Hinweis: Ein Bericht (RPT-Datei) kann nur *einer* Berichtsaufgabe zugeordnet werden.

Bericht anfordern

Um den Bericht anzuzeigen, fordern Sie einen Bericht bei einem Benutzer mit Berechtigungen zur Berichtsverwaltung an. Normalerweise müssen ein Systemadministrator oder ein anderer Benutzer mit Berichtsverwaltungsberechtigungen eine Berichtsanfrage genehmigen, bevor das System sie fertig stellt. Eine Genehmigung ist erforderlich, weil einige Berichte eine lange Zeit oder bedeutende Systemressourcen zur Ausführung benötigen können. Wenn Ihre Berichtsanfrage eine Genehmigung benötigt, sendet Ihnen das System eine E-Mail-Warnmeldung.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole als Benutzer mit Zugriffsrechten für die Berichtsaufgaben an.
2. Wählen Sie im Navigationsmenü "Berichte", "Berichtsaufgaben", "Bericht anfordern".

   Eine Liste der Berichte wird angezeigt.
3. Wählen Sie den Bericht aus, der angefordert werden soll.

   Ein Parameterfenster wird angezeigt.
4. Geben Sie die erforderlichen Parameterdaten ein.

   Hinweis: Wenn Sie einen Snapshot-Bericht ausführen und keine Snapshots für diesen Bericht vorhanden sind, müssen Sie zunächst einen Snapshot aufzeichnen.

   - Einige Berichte zeigen den Systemzustand an einem bestimmten Zeitpunkt. Wenn Sie diesen Typ Bericht anfordern, wählen Sie einen Zeitpunkt aus, für den Sie Berichtsdaten sehen möchten. Dieser Zeitpunkt wird *Snapshot* genannt.

     Hinweis: Die Snapshot-Daten und -Zeiten, die Sie wählen können, sind vorbestimmt. Normalerweise führt der Systemadministrator oder ein anderer Benutzer mit Berichtsverwaltungsrechten diese Snapshot-Konfiguration aus. Wenn keine Snapshots für den Bericht verfügbar sind, den Sie anfordern möchten, setzen Sie sich mit einem Systemadministrator in Verbindung.
   - Einige Berichte zeigen die Aktivität über einen Zeitraum. Die Titel für diese Berichte fangen üblicherweise mit dem Wort *Audit* an. Wenn Sie diesen Typ Bericht anfordern, wählen Sie einen Zeitraum aus, für den Sie Berichtsdaten sehen möchten. Zum Beispiel können Sie den Audit-Bericht über Kennwortzurücksetzungen für die letzten 30 Tage ausführen.
5. Klicken Sie auf "Bericht planen", und wählen Sie einen Ablaufplan für Ihren Bericht aus.

   Jetzt

   Gibt an, dass der Bericht sofort ausgeführt wird.

   Einmal

Gibt an, dass der Bericht einmal während eines bestimmten Zeitraums ausgeführt wird. Wählen Sie zum Generieren des Berichts die Start- und Endzeit sowie das Start- und Enddatum aus.

Hinweis: Ziehen Sie diese Option in Betracht, wenn der Bericht, den Sie anfordern, eine große Datenmenge benötigt. Um Systemressourcen zu sparen, sollten Sie eine Zeit mit geringer Systemaktivität wählen.

6. Klicken Sie auf "Senden".

   Die Berichtsanfrage wird gesendet. Je nach Umgebungskonfiguration wird die Anfrage sofort oder nach Genehmigung von einem Administrator ausgeführt.

Anzeigen des Berichts

Je nach Umgebungskonfiguration wird ein Bericht zur Anzeige verfügbar, wenn ein Administrator die Anfrage für diesen Bericht genehmigt hat. Wenn Ihre Berichtsanfrage eine Genehmigung benötigt, sendet Ihnen das System eine E-Mail-Warnung. Der Bericht, den Sie anzeigen möchten, wird in der Suchliste nicht angezeigt, bis er genehmigt wird.

Hinweis: Damit Sie unter Verwendung der Aufgabe "Meine Berichte anzeigen" in CA IdentityMinder Berichte anzeigen können, müssen Sie in Ihrem Browser Sitzungscookies von Drittanbietern zulassen.

Gehen Sie wie folgt vor:

1. Wechseln Sie in der Benutzerkonsole zu "Berichte", "Berichtsaufgaben", und klicken Sie auf "Meine Berichte anzeigen".
2. Suchen Sie den generierten Bericht, den Sie anzeigen möchten.

   Es werden sowohl Wiederholungsberichte als auch Instanzen von Berichten bei Bedarf angezeigt.

   Hinweis: Wenn der Status des Berichts "Ausstehend/Wiederholend" lautet, wird der Bericht nicht generiert und es kann länger dauern, den Bericht abzuschließen.
3. Wählen Sie den Bericht aus, der angezeigt werden soll.
4. (Optional) Klicken Sie oben links auf "Diesen Bericht exportieren", um den Bericht in den folgenden Formaten zu exportieren:
   - Crystal Reports
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) - nur Daten
   - Microsoft Excel (97-2003) - Bearbeitbar
   - Rich Text Format (RTF)
   - Getrennte Werte (CSV)
   - XML

Fehlerbehebung

Im folgenden Abschnitt werden Fehlerbehebungsthemen rund um die Berichterstellung beschrieben.

Beim Anzeigen eines Berichts wird der Benutzer zur Infoview-Anmeldeseite weitergeleitet

Wenn Sie in CA IdentityMinder einen Bericht anzeigen, werden Sie möglicherweise zur Infoview-Anmeldeseite von Business Objects weitergeleitet.

Anzeigen des Berichts bei Weiterleitung

1. Vergewissern Sie sich, dass Sie den voll-qualifizierten Domänennamen des CA-Berichtsservers (BusinessObjects) verwenden.
2. Klicken Sie mit der rechten Maustaste auf die Infoview-Anmeldeseite und wählen Sie "Quelle anzeigen" aus.
3. Suchen Sie die URL für den Bericht.
4. Kopieren Sie die URL und fügen Sie sie in ein neues Browser-Fenster ein.
5. Wenn der Bericht nicht angezeigt wird, verwenden Sie ein HTTP-Verfolgungsprogramm, um weitere Informationen zu erhalten.
6. Wenn der Bericht nicht angezeigt wird, versuchen Sie Folgendes, um die Browser-Einstellungen zu reparieren:
   - Lassen Sie Cookies von Drittanbietern zu.
   - Sitzungscookies zulassen.
   - Hochsicherheitseinstellungen entfernen.

Generieren von Benutzerkonten für mehr als 20.000 Datensätze

Wenn mehr als 20.000 Datensätze vorhanden sind, sind einige zusätzliche Schritte notwendig, um einen Benutzerkontenbericht zu generieren.

So generieren Sie einen Benutzerkontenbericht, wenn mehr als 20.000 Datensätze vorhanden sind

1. Öffnen Sie die zentrale Management-Konsole von Business Objects.
2. Klicken Sie auf Server und wählen Sie *Servername*.pageserver aus.
3. Wählen Sie für den Eintrag "Zu lesende Datenbank-Datensätze bei der Vorschau oder Aktualisierung eines Berichts" die Option "Unbegrenzte Datensätze" aus.
4. Öffnen Sie über den Crystal Reports-Designer den Benutzerkontenbericht.
5. Über die Datenbank-Option "Speicherort der Datenquelle festlegen" legen Sie den Datenbankspeicherort für Ihre Snapshot-Datenbank fest.
6. Diese Änderung speichern.

7. Klicken Sie in der Datenbank-Option "Datasource Expert" (Expert-Datenquelle) mit der rechten Maustaste im rechten Fenster auf "Befehl".

   Die SQL-Syntax wird links angezeigt. Außerdem wird die Parameterliste angezeigt.

8. Geben Sie den Parameternamen so ein, wie Sie ihn in den Parameterfeldern der Berichtsvorlage finden.

9. Ändern Sie die Abfrage auf der linken Seite, und fügen Sie diesen Parameter in der Abfrage hinzu.

   Wenn Sie beispielsweise den "reportid"-Parameter haben, wird die Abfrage folgende sein:

   ```
   Select *  from endPointAttributes, endpointview, imreport6
   where endPointAttributes.imr_endpointid = endpointview.imr_endpointid and
   endPointAttributes.imr_reportid = endpointview.imr_reportid
    endpointview.imr_reportid = imreport6.imr_reportid und imreport6.imr_reportid
   = {?reportid}
   ```

10. Den Bericht speichern.

Kapitel 15: Identitätsrichtlinien

Dieses Kapitel enthält folgende Themen:

Identitätsrichtlinien (siehe Seite 473)
Präventive Identitätsrichtlinien (siehe Seite 497)
Kombinieren von Identitätsrichtlinien und präventiven Identitätsrichtlinien (siehe Seite 508)

Identitätsrichtlinien

Eine Identitätsrichtlinie bezeichnet einen Satz von Geschäftsänderungen, die eintreten, wenn ein Benutzer eine bestimmte Bedingung oder Regel erfüllt. Mit Identitätsrichtliniensätzen können Sie folgende Schritte ausführen:

- Automatisieren bestimmter Identitätsmanagementaufgaben wie z. B. Zuweisen von Rollen und Gruppenmitgliedschaften, Zuordnen von Ressourcen oder Ändern von Attributen von Benutzerprofilen.
- Durchsetzen, dass Pflichten getrennt werden. Sie können z. B. einen Identitätsrichtliniensatz erstellen, der verhindert, dass Mitglieder der Rolle "Scheckunterzeichner" über die Rolle "Scheckgenehmiger" verfügen, und der für alle Angehörigen der Firma das Ausstellen von Schecks auf $10.000 beschränkt.
- Konformität durchsetzen. Sie können z. B. Benutzer überprüfen, die einen bestimmten Titel haben und mehr als $100.000 verdienen.

  Identitätsrichtlinien, die für Konformität sorgen, werden als *Konformitätsrichtlinien* bezeichnet.

Die Geschäftsänderungen, die mit einer Identitätsrichtlinie verknüpft sind, umfassen:

- Das Zuweisen oder Widerrufen von Rollen einschließlich Bereitstellungsrollen (wenn Sie nur ein Bereitstellungsverzeichnis verwenden)
- Zuweisen oder Entziehen einer Gruppenmitgliedschaft
- Aktualisieren der Attribute in einem Benutzerprofil

Eine Firma kann z. B. möglicherweise eine Identitätsrichtlinie erstellen, die angibt, dass alle stellvertretenden Vorsitzenden zu der Gruppe "Country-Club-Mitglied" gehören und über die Rolle "Gehaltsgenehmiger" verfügen. Wenn sich der Titel eines Benutzers in "stellvertretender Vorsitzender" ändert und dieser Benutzer mit der Identitätsrichtlinie synchronisiert wird, fügt CA IdentityMinder den Benutzer zu der entsprechenden Gruppe und Rolle hinzu. Wenn ein stellvertretender Vorsitzender zum Vorstandsvorsitzenden befördert wird, erfüllt er oder sie die Bedingung in der Identitätsrichtlinie "stellvertretender Vorsitzender" nicht mehr. Daher werden die durch diese Richtlinien übernommenen Änderungen widerrufen, und es werden neue Änderungen basierend auf der Vorstandsvorsitzenden-Richtlinie übernommen.

Die Änderungsaktionen, die basierend auf einer Identitätsrichtlinie ausgeführt werden, enthalten Ereignisse, die unter Workflow-Steuerung gestellt und überprüft werden können. Im vorhergehenden Beispiel gewährt die Rolle "Gehaltsgenehmiger" ihren Mitgliedern weitreichende Berechtigungen. Um die Rolle "Gehaltsgenehmiger" zu schützen, kann die Firma einen Workflow-Prozess erstellen, der einen Satz von Genehmigungen erfordert, bevor die Rolle zugewiesen wird. Außerdem kann sie CA IdentityMinder so konfigurieren, dass er die Zuweisung der Rolle überprüft.

Zur Vereinfachung des Identitätsrichtlinienmanagements sind Identitätsrichtlinien in einem Identitätsrichtliniensatz gruppiert. Die Richtlinien "stellvertretender Vorsitzender" und "Vorstandsvorsitzender" können z. B. Teil des Identitätsrichtliniensatzes "Führungskräfteberechtigungen" sein.

Hinweis: CA IdentityMinder enthält einen weiteren Identitätsrichtlinientyp, der *präventive Identitätsrichtlinie* (siehe Seite 497) genannt wird. Diese Richtlinien werden vor dem Senden einer Aufgabe ausgeführt. Mit ihnen kann ein Administrator nach Richtlinienverletzungen suchen, bevor er Berechtigungen zuweist oder Profilattribute ändert. Wenn eine Verletzung vorliegt, kann sie der Administrator beheben, bevor er die Aufgabe sendet.

Arbeitsblatt zum Planen von Identitätsrichtliniensätzen

Ein Identitätsrichtliniensatz enthält eine oder mehrere Identitätsrichtlinien. Verwenden Sie das folgende Arbeitsblatt, um alle Identitätsrichtlinien in dem Satz zu planen, bevor Sie einen Identitätsrichtliniensatz erstellen.

Frage	Ihre Antwort
Wie möchten Sie die Identitätsrichtlinie nennen?	
Für welche Benutzer soll die Identitätsrichtlinie übernommen werden?	

Frage	Ihre Antwort
Welche Aktionen soll CA IdentityMinder ausführen, wenn eine Identitätsrichtlinie für einen Benutzer übernommen wird?	
Welche Aktionen soll CA IdentityMinder ausführen, wenn eine Identitätsrichtlinie, die einmal für einen Benutzer übernommen wurde, nicht mehr gilt?	
Soll CA IdentityMinder die Änderungen in einer Identitätsrichtlinie mehrmals anwenden oder nur, wenn ein Benutzer die Bedingungen in der Richtlinie zum ersten Mal erfüllt?	

Nachdem Sie dieses Arbeitsblatt für jede Identitätsrichtlinie in einem Richtliniensatz ausgefüllt haben, verifizieren Sie, dass die Richtlinien nicht mit anderen Richtlinien in Konflikt stehen. Stellen Sie z. B. sicher, dass eine Richtlinie keine Berechtigung gewährt, die eine andere Richtlinie widerruft.

Erstellen eines neuen Identitätsrichtliniensatzes

Sie müssen über die Rolle "System-Manager" oder eine Rolle verfügen, die die Aufgabe "Identitätsrichtliniensatz erstellen" enthält, um einen Identitätsrichtliniensatz zu erstellen.

Führen Sie die folgenden Schritte aus, um einen Identitätsrichtliniensatz zu erstellen:

1. Definieren Sie das Profil für den Identitätsrichtliniensatz (siehe Seite 476)
2. Erstellen Sie eine Richtliniensatz-Mitgliedsregel (siehe Seite 477)
3. Erstellen Sie eine Identitätsrichtlinie (siehe Seite 477)
4. Geben Sie die Eigentümer für den Identitätsrichtliniensatz an (siehe Seite 487)

Hinweis: Um Richtlinien für eine CA IdentityMinder-Umgebung zu verwenden, aktivieren Sie Identitätsrichtlinien in der Management-Konsole für CA IdentityMinder. Weitere Informationen finden Sie im *Konfigurationshandbuch.*

Definieren Sie das Profil für den Identitätsrichtliniensatz

Sie können grundlegende Eigenschaften für einen Identitätsrichtliniensatz über die Registerkarte "Profil" definieren.

So definieren Sie ein Profil für einen Identitätsrichtliniensatz:

1. Wählen Sie in der Benutzerkonsole "Richtlinien", "Identitätsrichtlinien verwalten", "Identitätsrichtliniensatz erstellen" aus.

   Sie müssen als Benutzer mit Berechtigungen bei CA IdentityMinder angemeldet sein, um Identitätsrichtlinien zu verwalten. Die Standardrolle "System-Manager" verfügt über diese Berechtigungen.

2. Entscheiden Sie, ob Sie einen neuen Identitätsrichtliniensatz oder eine Kopie eines vorhandenen Identitätsrichtliniensatzes erstellen möchten.
3. Geben Sie einen Namen für den Identitätsrichtliniensatz ein.
4. Geben Sie eine Kategorie für den Identitätsrichtliniensatz ein.

   Die Kategorie gruppiert Identitätsrichtliniensätze für ähnliche Zwecke zur Berichterstellung. Die Verwendung des Felds "Kategorie" ist obligatorisch.

5. Geben Sie optional eine Beschreibung für den Identitätsrichtliniensatz ein.
6. Wenn Sie den Identitätsrichtliniensatz nicht zur Verwendung verfügbar machen möchten, deaktivieren Sie das Kontrollkästchen "Aktiviert".
7. Wenn Sie die Registerkarte "Profil" ausgefüllt haben, wählen Sie die Registerkarte "Richtlinien" aus, um die Identitätsrichtlinien für den Identitätsrichtliniensatz zu erstellen.

Weitere Informationen:

Erstellen Sie eine Identitätsrichtlinie (siehe Seite 477)
Erstellen Sie eine Richtliniensatz-Mitgliedsregel (siehe Seite 477)

Erstellen Sie eine Richtliniensatz-Mitgliedsregel

Sie können eine Mitgliederregel für einen Richtliniensatz erstellen, so dass der Richtliniensatz nur für bestimmte Benutzer gilt. Die Regel wird vor Identitätsrichtlinien im Satz ausgewertet, wodurch eine erhebliche Zeitersparnis möglich ist. Wenn eine Mitgliedsregel die Auswertung der Identitätsrichtlinie beispielsweise auf 10 Prozent der Benutzer beschränkt, verringert die Regel die Auswertungszeit um 90 Prozent.

So erstellen Sie eine Richtliniensatz-Mitgliedsregel

1. Wählen Sie die Registerkarte "Richtlinien" aus.
2. Klicken Sie unter "Richtliniensatz-Mitgliedsregel" auf das Symbol "Bearbeiten".
3. Geben Sie eine Regel ein, so dass die Richtlinie nur für bestimmte Benutzer gilt.
4. Klicken Sie auf "OK".

Weitere Informationen

Erstellen Sie eine Identitätsrichtlinie (siehe Seite 477)

Erstellen Sie eine Identitätsrichtlinie

Nachdem Sie das Profil und die Mitgliederregel für den Identitätsrichtliniensatz definiert haben, können Sie die Identitätsrichtlinien in diesem Richtliniensatz definieren.

Hinweis: In umfangreichen Implementierungen kann die Auswertung von Identitätsrichtlinienregeln erhebliche Zeit in Anspruch nehmen. Sie können die Auswertungszeit für Regeln mit Benutzerattributen verkürzen, indem Sie die Option für die Auswertung im Arbeitsspeicher aktivieren. Weitere Informationen finden Sie im *Konfigurationshandbuch*.

So erstellen Sie eine Identitätsrichtlinie

1. Wählen Sie die Registerkarte "Richtlinien" aus.
2. Klicken Sie auf "Hinzufügen".
3. Geben Sie einen Namen für die Identitätsrichtlinie ein.
4. Wählen Sie das Kontrollkästchen "Einmal übernehmen" aus, wenn die Richtlinie nur übernommen werden sollen, wenn ein Benutzer die Richtlinie zum ersten Mal erfüllt.

5. Wählen Sie das Kontrollkästchen "Konformität" aus, um diese Richtlinie als Konformitätsrichtlinie zu kennzeichnen.

   Wenn dieses Kontrollkästchen ausgewählt wird:

   - CA IdentityMinder kann Berichte für Benutzer erstellen, die nicht mit Konformitätsrichtlinien synchronisiert sind.
   - Die Aktion "Konformitätsverletzung" wird in dem Listenfeld der Aktion zu "Richtlinie übernehmen/entfernen" angezeigt.

6. Identifizieren Sie die Benutzer, für die die Richtlinie gilt, im Abschnitt "Richtlinienbedingung".
7. Definieren Sie in dem Abschnitt der Aktion zu "Richtlinie übernehmen" die Aktionen, die CA IdentityMinder ausführen soll, wenn die Identitätsrichtlinie für einen Benutzer übernommen wird.
8. Definieren Sie in dem Abschnitt der Aktion "Richtlinie entfernen" die Aktionen, die CA IdentityMinder ausführen soll, wenn ein Benutzer die Bedingungen für die Identitätsrichtlinie nicht mehr erfüllt.
9. Klicken Sie auf "OK".

Hinweis: Bevor Sie den Identitätsrichtliniensatz, den Sie erstellt haben, verwenden können, müssen Sie in der Management-Konsole Identitätsrichtlinien aktivieren. Weitere Informationen finden Sie im *Konfigurationshandbuch.*

Die Einstellung "Einmal übernehmen"

CA IdentityMinder übernimmt eine Identitätsrichtlinie basierend auf der Einstellung "Einmal übernehmen" unterschiedlich.

Aktivieren der Einstellung "Einmal übernehmen"

Wenn die Einstellung "Einmal übernehmen" aktiviert ist, übernimmt CA IdentityMinder die mit der Identitätsrichtlinie verknüpften Änderungen, wenn ein Benutzer die in der Richtlinie definierte Bedingung *zum ersten Mal* erfüllt. Die mit der Richtlinie verknüpften Änderungsaktionen finden nur einmal statt. Daher übernimmt CA IdentityMinder Richtlinienaktualisierungen nicht für Benutzer, wenn die Richtlinie zuvor übernommen worden war.

Wenn ein Benutzer die in der Richtlinie definierte Bedingung nicht mehr erfüllt, führt CA IdentityMinder die Aktion "Entfernen" der Richtlinie aus.

Die Einstellung "Einmal übernehmen" wird üblicherweise verwendet, wenn Ressourcen bereitgestellt werden. Sie verfügen z. B. möglicherweise über eine Richtlinie, die Managern ein Mobiltelefon zuweist. Wenn ein Benutzer ein Manager wird, wird diesem Benutzer ein Mobiltelefon zugewiesen. CA IdentityMinder gibt das Mobiltelefon nur einmal aus, nicht jedes Mal, wenn die Richtlinie ausgewertet wird. Wenn die Mobiltelefonrichtlinie mit einem neueren Mobiltelefonmodell aktualisiert wird, gibt CA IdentityMinder keine neuen Mobiltelefone an bestehende Manager aus.

Hinweis: Ressourcenbereitstellung ist verfügbar, wenn CA IdentityMinder in einen Bereitstellungsserver integriert ist.

Deaktivieren der Einstellung "Einmal übernehmen"

Wenn die Einstellung "Einmal übernehmen" nicht aktiviert ist, werden die mit der Identitätsrichtlinie verknüpften Änderungsaktionen jedes Mal übernommen, wenn eine Identitätsrichtlinie ausgewertet wird. Dies bedeutet, dass CA IdentityMinder Änderungsaktionen für jeden Benutzer übernimmt, der die Bedingungen in der Richtlinie erfüllt, unabhängig davon, ob die Änderungsaktionen zuvor übernommen worden waren.

Üblicherweise deaktivieren Sie die Einstellung "Einmal übernehmen" in einer Identitätsrichtlinie, die Konformität durchsetzt. Sie können z. B. eine Identitätsrichtlinie erstellen, die die Ausgabenbefugnis von Managern auf $ 5.000 beschränkt. Wenn CA IdentityMinder einen Manager findet, dessen Ausgabenbefugnis auf $ 10.000 eingestellt ist, setzt er die Ausgabenbefugnis auf $ 5.000 zurück. Immer, wenn ein Manager mit der Identitätsrichtlinie synchronisiert wird, stellt CA IdentityMinder sicher, dass die Ausgabenbefugnis ordnungsgemäß eingestellt ist.

Wenn an einem Benutzerprofil eine manuelle Änderung vorgenommen wird, die mit einer Änderungsaktion in Konflikt steht, überschreibt CA IdentityMinder die Änderung, wenn der Benutzer mit der Richtlinie synchronisiert wird.

Wenn im vorhergehenden Beispiel die Ausgabenbefugnis eines Managers auf $ 10.000 erhöht wird, setzt CA IdentityMinder die Ausgabenbefugnis auf $ 5.000 zurück, wenn der Manager mit der Richtlinie synchronisiert wird.

Die folgende Tabelle enthält eine Zusammenfassung der Auswirkungen des Aktivierens oder Deaktivierens der Einstellung "Einmal übernehmen".

Wenn "Einmal übernehmen" so eingestellt ist:	Dann...
Aktiviert	■ werden Änderungsaktionen, die mit der Identitätsrichtlinie verknüpft sind, nur einmal übernommen ■ bleiben manuelle Änderungen, die vorgenommen werden, nachdem die Identitätsrichtlinie übernommen worden ist, erhalten ■ werden Aktualisierungen nicht für Benutzer übernommen, die die Bedingung in einer Identitätsrichtlinie erfüllen, wenn CA IdentityMinder die Richtlinie zuvor übernommen hat ■ führt CA IdentityMinder die Aktionen "Entfernen" aus, wenn ein Benutzer die Bedingung in einer Identitätsrichtlinie nicht mehr erfüllt
Deaktiviert	■ werden mit der Identitätsrichtlinie verknüpfte Änderungsaktionen jedes Mal übernommen, wenn ein Benutzer mit der Richtlinie synchronisiert wird ■ werden manuelle Änderungen überschrieben, wenn die Identitätsrichtlinie übernommen wird ■ werden Aktualisierungen der Richtlinie übernommen, wenn ein Benutzer synchronisiert wird ■ führt CA IdentityMinder die Aktionen "Entfernen" aus, wenn ein Benutzer die Bedingung in einer Identitätsrichtlinie nicht mehr erfüllt

Richtlinienbedingungen

Richtlinienbedingungen sind die Regeln, die die Gruppe der Benutzer festlegen, für die eine Identitätsrichtlinie gilt.

In der folgenden Tabelle werden die zur Verfügung stehenden Optionen beschrieben.

Syntax	Bedingung	Beispiel
(Alle)	Die Identitätsrichtlinie gilt für alle Benutzer.	
wobei <Benutzerfilter>	Der Benutzer muss mit einem oder mehreren Attributwerten übereinstimmen.	Benutzer wobei Titel=Manager und Standort=Ost

Syntax	Bedingung	Beispiel
in <Org-Regel>	Der Benutzer muss den bezeichneten Organisationen angehören. **Hinweis:** Wenn Sie diese Option auswählen, zeigt CA IdentityMinder ein neues Listenfeld an, aus dem Sie die folgenden Optionen auswählen können: ■ Organisation <Organisation> [und niedriger]: Verwenden Sie ein Organisationssuchfenster, um eine Organisation auszuwählen und schließen Sie optional die Unterorganisationen der Organisation ein. ■ Organisationen, bei denen <Org-Filter> [und niedriger] zutrifft: Geben Sie einen Filter an, der eine oder mehrere Organisationen auswählt.	Benutzer in Organisation Vertrieb und niedriger
wobei <Benutzerfilter> und sind in <Org-Regel>	Der Benutzer muss mit den spezifischen Benutzerattributen übereinstimmen und zu einer bestimmten Organisation gehören.	Titel=Manager und Organisation=Vertrieb*
als Mitglieder von <Gruppenmitgliedsregel>	Der Benutzer muss einer Gruppe angehören, die eine Bedingung erfüllt, welche von den Attributen der Gruppe festgelegt werden. **Hinweis:** Wenn Sie diese Option auswählen, zeigt CA IdentityMinder ein neues Listenfeld an, aus dem Sie die folgenden Optionen auswählen können: ■ Gruppe <Gruppe> – Verwenden Sie ein Gruppensuchfenster, um eine Gruppe auszuwählen. ■ Gruppe, bei der <Gruppenfilter> zutrifft: Geben Sie einen Filter an, der eine oder mehrere Gruppen auswählt.	Benutzer als Mitglieder von Gruppen, bei denen Eigentümer=CIO

Syntax	Bedingung	Beispiel
als Mitglieder von <Rollenregel>	Der Benutzer muss Mitglied der Rolle sein. Bei der Rolle kann es sich um folgende handeln: ■ Zugriffsrolle ■ Admin-Rolle ■ Bereitstellungsrolle **Hinweis:** Um Bereitstellungsrollen zu verwenden, muss CA IdentityMinder in einen Bereitstellungsserver integriert sein. Weitere Informationen finden Sie im *Installationshandbuch.*	Benutzer als Mitglieder von Helpdesk Rolle
als Administratoren von <Rollenregel>	Der Benutzer muss ein Administrator für eine Rolle sein. Bei der Rolle kann es sich um folgende handeln: ■ Zugriffsrolle ■ Admin-Rolle ■ Bereitstellungsrolle **Hinweis:** Um Bereitstellungsrollen zu verwenden, muss CA IdentityMinder in einen Bereitstellungsserver integriert sein. Weitere Informationen finden Sie im *Installationshandbuch.*	Benutzer als Administratoren von Vertriebs-Manager Rolle
als Eigentümer von <Rollenregel>	Der Benutzer muss Eigentümer einer Rolle sein. Bei der Rolle kann es sich um folgende handeln: ■ Zugriffsrolle ■ Admin-Rolle ■ Bereitstellungsrolle **Hinweis:** Um Bereitstellungsrollen zu verwenden, muss CA IdentityMinder in einen Bereitstellungsserver integriert sein. Weitere Informationen finden Sie im *Installationshandbuch.*	Benutzer als Eigentümer von Benutzer-Manager Rolle
von der Abfrage zurückgegeben <LDAP-Abfrage>	Der Benutzer muss eine Bedingung auf Grundlage einer LDAP-Anfrage erfüllen.	Benutzer, die die Bedingungen einer LDAP-Abfrage erfüllen. Beispielsweise: (departmentNumber=Konten)

Syntax	Bedingung	Beispiel
in <administrative-Vereinigungsmengen-Beschränkung>	Der Benutzer muss zumindest eine der Bedingungen aus einer Liste der Bedingungen erfüllen. Sie können die folgenden Filtertypen in eine administrative Vereinigungsmengen-Beschränkung aufnehmen: ■ Mitglied einer Zugriffs-/Admin-/Bereitstellungsrolle ■ Administrator einer Zugriffs-/Admin-/Bereitstellungsrolle ■ Eigentümer einer Zugriffs-/Admin-/Bereitstellungsrolle ■ Mitglied einer Gruppe	Benutzer, die Mitglied der Rolle "Manager zertifizieren" *oder* die Eigentümer der Rolle "Manager zertifizieren" sind.
in <administrative-Schnittmengen-Beschränkung>	Der Benutzer muss alle Bedingungen in einer Liste der Bedingungen erfüllen. Sie können die folgenden Filtertypen in eine administrative Vereinigungsmengen-Beschränkung aufnehmen: ■ Mitglied einer Zugriffs-/Admin-/Bereitstellungsrolle ■ Administrator einer Zugriffs-/Admin-/Bereitstellungsrolle ■ Eigentümer einer Zugriffs-/Admin-/Bereitstellungsrolle ■ Mitglied einer Gruppe	Benutzer, die Mitglieder der Rolle "Vertragsinitiator" *und* der Rolle "Vertragsgenehmiger" sind.

Aktionen zu "Richtlinien anwenden/entfernen"

Sie können Änderungsaktionen definieren, die CA IdentityMinder ausführt, wenn er die Identitätsrichtlinie auswertet. Die Aktionen umfassen:

Aktionen zu "Richtlinie anwenden"

Ein Satz von Aktionen, die CA IdentityMinder ausführt, wenn ein Benutzer die Bedingungen in den Richtlinienbedingungen erfüllt.

Aktionen zu "Richtlinie entfernen"

Ein Satz von Aktionen, die CA IdentityMinder ausführt, wenn ein Benutzer die Bedingungen in den Richtlinienbedingungen nicht mehr erfüllt.

Die Aktionen, die CA IdentityMinder ausführen kann, wenn Identitätsrichtlinien übernommen oder entfernt werden, sind identisch. Weitere Informationen finden Sie in der folgenden Tabelle.

Änderungsaktion:	**Beschreibung**
Zur Gruppe <Gruppenname> hinzufügen [...]	Dient zum Hinzufügen eines Benutzers zu einer Gruppe. Wenn Sie diese Aktion auswählen, stellt CA IdentityMinder ein Fenster dar, in dem Sie nach der gewünschten Gruppe suchen können.
Zu <Gruppenname> in der Organisation des Benutzers hinzufügen	Dient zum Hinzufügen eines Benutzers zu einer lokalen Gruppe. Wenn Sie diese Option auswählen, stellt CA IdentityMinder ein Textfeld dar, in das Sie den Namen der gewünschten Gruppe eingeben können.
<Benutzerattribut-mit-einem-Wert> auf <Wert> stellen	Legt den Wert eines Attributs in einem Benutzerprofil fest. Falls ein Wert vorhanden ist, überschreibt CA IdentityMinder ihn mit dem in der Änderungsaktion angegebenen Wert.
<Wert> zu <Mehrfachwert-Benutzerattribut> hinzufügen	Dient zum Hinzufügen eines Werts zu einem Mehrfachwertbenutzerattribut. Diese Option überschreibt keine vorhandenen Werte.
Zum Mitglied von Zugriffsrolle machen	Dient zum Zuweisen von Benutzern zu einer Zugriffsrolle.
Zum Administrator von Zugriffsrolle machen	Dient dazu, Benutzer zu Administratoren einer Zugriffsrolle zu machen
Zum Mitglied von Admin-Rolle machen	Dient dazu, Benutzer zu Mitgliedern einer Admin-Rolle zu machen
Zum Administrator von Admin-Rolle machen	Dient dazu, Benutzer zu Administratoren einer Admin-Rolle zu machen
Zum Mitglied der Bereitstellungsrolle machen	Dient dazu, Benutzer zu Mitgliedern einer Bereitstellungsrolle zu machen, die verknüpfte Endpunktkonten erstellt. **Hinweis:** Um Bereitstellungsrollen zu verwenden, muss CA IdentityMinder in einen Bereitstellungsserver integriert sein. Informationen hierzu finden Sie im *Installationshandbuch* für Ihren Anwendungsserver.
Zum Administrator der Bereitstellungsrolle machen	Dient dazu, Benutzer zu Administratoren einer Bereitstellungsrolle zu machen. **Hinweis:** Um Bereitstellungsrollen zu verwenden, muss CA IdentityMinder in einen Bereitstellungsserver integriert sein. Informationen hierzu finden Sie im *Installationshandbuch* für Ihren Anwendungsserver.

Änderungsaktion:	Beschreibung
Aus Gruppe <Gruppenname> entfernen [...]	Dient zum Entfernen von Benutzern aus einer Gruppe. Wenn Sie diese Aktion auswählen, stellt CA IdentityMinder ein Fenster dar, in dem Sie nach der gewünschten Gruppe suchen können.
Aus <Gruppenname> in Organisation des Benutzers entfernen	Dient zum Entfernen von Benutzern aus einer lokalen Gruppe. Wenn Sie diese Option auswählen, stellt CA IdentityMinder ein Textfeld dar, in das Sie den Namen der gewünschten Gruppe eingeben können.
<Wert> aus <Mehrwertbenutzerattribut> entfernen	Dient zum Entfernen eines Werts aus einem Mehrwertbenutzerattribut.
Mitglied aus Zugriffsrolle entfernen	Dient zum Widerrufen einer Zugriffsrolle.
Administrator aus Zugriffsrolle entfernen	Dient zum Widerrufen von Administratorberechtigungen für eine bestimmte Zugriffsrolle
Mitglied aus Admin-Rolle entfernen	Dient zum Widerrufen einer Admin-Rolle.
Administrator aus Admin-Rolle entfernen	Dient zum Widerrufen von Administratorberechtigungen für eine bestimmte Admin-Rolle
Mitglied aus der Bereitstellungsrolle entfernen	Dient zum Widerrufen einer Bereitstellungsrolle.
Administrator aus der Bereitstellungsrolle entfernen	Dient zum Widerrufen von Administratorberechtigungen für eine bestimmte Bereitstellungsrolle.
Überprüfungsmeldung senden	Dient zum Senden einer von Ihnen erstellten Nachricht an die Audit-Datenbank. Diese Nachricht kann in einem Bericht angezeigt werden, den Sie erstellen.
Konformitätsverletzung	Dient zum Senden einer von Ihnen erstellten Nachricht an die Audit-Datenbank. Wenn Sie einen Konformitätsbericht erstellen, wird die Nachricht jedes Mal angezeigt, wenn die Identitätsrichtlinie übernommen oder aus einem Benutzer entfernt wird. Weitere Informationen zur Überprüfung finden Sie im *Konfigurationshandbuch.* **Hinweis:** Sie müssen das Kontrollkästchen "Konformität" auf der Registerkarte "Profil" aktivieren, damit der Identitätsrichtliniensatz die Option "Konformitätsverletzung" verwendet.

Änderungsaktion:	Beschreibung
Akzeptieren (nur Aktion zu "Richtlinie anwenden")	Mit dieser Aktion kann die Aufgabe gesendet werden, wenn eine Verletzung der präventiven Identitätsrichtlinie vorliegt. Wenn Sie diese Aktion auswählen, stellen Sie eine Meldung bereit, die CA IdentityMinder in die Audit-Datenbank schreibt und unter "Gesendete Aufgaben anzeigen" anzeigt, wenn eine Verletzung auftritt.
Ablehnen (nur Aktion zu "Richtlinie anwenden")	Verhindert, dass eine Aufgabe sendet, wenn eine Verletzung der Identitätsrichtlinie vorliegt. Diese Aktion wird mit präventiven Identitätsrichtlinien verwendet, damit Benutzer keine Berechtigungen erhalten, die zu einem Interessenkonflikt führen oder für einen Betrug verwendet werden können. Wenn Sie diese Aktion auswählen, können Sie auch eine Meldung bereitstellen, die CA IdentityMinder bei einer Verletzung anzeigt. Die Meldung wird in der Audit-Datenbank gespeichert und in der Benutzerkonsole angezeigt.
Warnung (nur Aktion zu "Richtlinie anwenden")	Löst einen Workflow-Prozess aus, wenn eine präventive Identitätsrichtlinie verletzt wird, wenn Sie diese Verletzung mit einer Workflow-Genehmigungsrichtlinie verbinden. CA IdentityMinder erlaubt der Aufgabe das Senden, unabhängig davon, ob ein Workflow konfiguriert ist. **Hinweis:** Informationen zum Verknüpfen eines Workflow-Prozesses mit einer präventiven Identitätsrichtlinie finden Sie unter Workflow und präventive Identitätsrichtlinien (siehe Seite 503). Wenn Sie diese Aktion auswählen, können Sie auch eine Meldung bereitstellen, die CA IdentityMinder bei einer Verletzung anzeigt. Die Meldung wird in der Audit-Datenbank gespeichert und unter "Gesendete Aufgaben anzeigen" angezeigt.

Weitere Informationen:

Präventive Identitätsrichtlinien (siehe Seite 497)
Workflow und präventive Identitätsrichtlinien (siehe Seite 503)

Geben Sie die Eigentümer für den Identitätsrichtliniensatz an

Definieren Sie auf der Registerkarte "Eigentümer" Regeln dafür, wer Eigentümer des Identitätsrichtliniensatzes sein kann. Ein Eigentümer eines Identitätsrichtliniensatzes kann die grundlegenden Informationen über den Richtliniensatz ändern und kann Identitätsrichtlinien zu dem Satz hinzufügen, sie darin ändern oder aus ihm entfernen.

So vervollständigen Sie die Registerkarte "Eigentümer":

1. Definieren Sie Eigentümerregeln, die bestimmen, welche Benutzer den Identitätsrichtliniensatz ändern können.
2. Klicken Sie auf "Senden".

Verwalten eines neuen Identitätsrichtliniensatzes

CA IdentityMinder umfasst die folgenden Aufgaben zum Verwalten eines Identitätsrichtliniensatzes:

- Identitätsrichtliniensatz anzeigen
- Identitätsrichtliniensatz ändern
- Identitätsrichtliniensatz löschen

Wenn ein Administrator eine dieser Aufgaben anwendet, zeigt CA IdentityMinder standardmäßig eine Liste aller Identitätsrichtliniensätze an, deren Eigentümer dieser Administrator ist. Der Administrator kann dann den erforderlichen Richtliniensatz aus der Liste auswählen.

In einer Identity Manager-Umgebung, die viele Identitätsrichtliniensätze enthält, möchten Sie möglicherweise die Aufgaben "Identitätsrichtliniensatz anzeigen", "Identitätsrichtliniensatz ändern" und "Identitätsrichtliniensatz löschen" anpassen, damit Administratoren nach einem Identitätsrichtliniensatz suchen können, statt sie in einer Liste anzuzeigen.

So passen Sie diese Aufgaben an:

1. Wählen Sie in der Benutzerkonsole die Optionen "Rollen und Aufgaben", "Admin-Rollen", "Admin-Aufgabe ändern" aus.

   Das Fenster "Admin-Aufgabe ändern" öffnet sich.
2. Suchen Sie die Aufgabe, die Sie anpassen möchten, und wählen Sie sie aus.
3. Wählen Sie auf der Registerkarte "Bereich" die Option "Alle Identitätsrichtliniensätze" aus.

   Wenn Sie diese Option auswählen, verwendet CA IdentityMinder die Fensterdefinition "Standardsuche: Identitätsrichtliniensätze".
4. Klicken Sie auf "Submit".

Synchronisieren von Benutzern und Identitätsrichtlinien

Beim Verwenden von Identitätsrichtlinien sollten Sie damit vertraut sein, wie CA IdentityMinder die Richtlinien auswertet und für Benutzer anwendet. Ohne genaue Kenntnisse der Benutzersynchronisierung konfigurieren Sie möglicherweise Identitätsrichtliniensätze, die zu unerwarteten Ergebnissen führen.

Das folgende Verfahren erläutert, wie CA IdentityMinder Identitätsrichtlinien auswertet und sie anwendet:

1. Der Benutzersynchronisierungsdurchlauf beginnt:
   - **Automatisch**: Sie können Aufgaben von CA IdentityMinder so konfigurieren, dass sie die Benutzersynchronisierung automatisch auslösen
   - **Manuell**: Mit Hilfe der Aufgabe "Benutzer synchronisieren" in der Benutzerkonsole können Sie einen Benutzer synchronisieren.
2. CA IdentityMinder ermittelt die Identitätsrichtlinien, die für einen Benutzer gelten.
3. CA IdentityMinder vergleicht die Identitätsrichtlinien, die für einen Benutzer gelten, mit der Liste der Richtlinien, die bereits für diesen Benutzer übernommen wurden.

   Hinweis: Die Liste der Richtlinien, die bereits für einen Benutzer übernommen wurden, sind im bekannten Attribut %IDENTITY_POLICY% im Benutzerprofil gespeichert. Informationen über das Konfigurieren dieses Attributs finden Sie im *Konfigurationshandbuch*.

   - Falls eine Identitätsrichtlinie in der Liste der anwendbaren Richtlinien aufgeführt wird *und* diese Richtlinie zuvor *nicht* für den Benutzer übernommen wurde, fügt CA IdentityMinder sie zu einer Zuweisungsliste hinzu.
   - Falls eine Identitätsrichtlinie in der Liste der anwendbaren Richtlinien aufgeführt wird, diese Richtlinie bereits für den Benutzer übernommen wurde und die Einstellung "Einmal übernehmen" deaktiviert ist, fügt CA IdentityMinder sie zur Liste der Richtlinien, die erneut zugewiesen werden, hinzu.
   - Wenn eine Identitätsrichtlinie nicht in der Liste der anwendbaren Richtlinien enthalten ist und die Richtlinie für den Benutzer übernommen wurde, stimmt der Benutzer nicht mehr mit der Richtlinienbedingung überein. CA IdentityMinder fügt diese Richtlinien zu einer Liste der Richtlinien, deren Zuweisung aufgehoben wird, hinzu.
4. Nachdem CA IdentityMinder alle Richtlinien eines Benutzers ausgewertet hat, werden diese in der folgenden Reihenfolge übernommen:
   a. Identitätsrichtlinien aus der Liste der Richtlinien, deren Zuweisung aufgehoben wird
   b. Identitätsrichtlinien aus der Liste der Richtlinien, die zugewiesen werden
   c. Identitätsrichtlinien aus der Liste der Richtlinien, die neu zugewiesen werden

5. Nachdem die Identitätsrichtlinien übernommen wurden, wertet CA IdentityMinder die Richtlinien erneut aus, um festzustellen, ob infolge der Änderungen, die während des ersten Synchronisierungsdurchlaufs (Schritte 2-4) vorgenommen wurden, weitere Änderungen erforderlich sind.

   Dadurch soll sichergestellt werden, dass die durch die Anwendung von Identitätsrichtlinien vorgenommenen Änderungen nicht andere Identitätsrichtlinien auslösen.

6. CA IdentityMinder wertet weiterhin Identitätsrichtlinien aus und übernimmt sie, bis der Benutzer mit allen anwendbaren Richtlinien synchronisiert ist oder bis CA IdentityMinder die höchste Rekursionsebene erreicht, die in der Management-Konsole definiert ist.

   Zum Beispiel ändert eine Identitätsrichtlinie möglicherweise die Abteilung eines Benutzers, wenn diesem eine Rolle zugewiesen wird. Die neue Abteilung löst eine andere Identitätsrichtlinie aus. Falls die Rekursionsebene jedoch auf 1 eingestellt ist, wird die nächste Änderung erst durchgeführt, nachdem der Benutzer wieder synchronisiert wurde.

   Weitere Informationen über das Einstellen der Rekursionsebene finden Sie in der Online-Hilfe zur Management-Konsole.

Konfigurieren der automatischen Benutzersynchronisierung

CA IdentityMinder kann Benutzerkonten an verschiedenen Punkten während des Bestehens einer Aufgabe automatisch mit Identitätsrichtlinien synchronisieren.

Eine Aufgabe von CA IdentityMinder erstellt *Ereignisse*, erkennbare Aktivitäten, die während der Aufgabenverarbeitung auftreten. Die Standardaufgabe "Benutzer erstellen" erstellt z. B. das CreateUserEvent, das AddUserToGroupEvent und das AssignAccessRoleEvent. Sie können CA IdentityMinder so konfigurieren, dass er Benutzer nach Abschluss einer Aufgabe oder nach Abschluss eines Ereignisses synchronisiert.

Hinweis: Im Abschnitt Synchronisieren von Benutzern mit Identitätsrichtlinien (siehe Seite 488) finden sie weitere Informationen über den Benutzersynchronisierungsdurchlauf.

So konfigurieren Sie eine Aufgabe so, dass sie die Benutzersynchronisierung auslöst

1. Melden Sie sich bei CA IdentityMinder als Benutzer an, der Admin-Aufgaben ändern kann.
2. Wählen Sie die Option "Rollen und Aufgaben" und dann die Option "Admin-Aufgaben" aus. Wählen Sie dann die Option "Admin-Aufgaben ändern" aus.

   CA IdentityMinder zeigt ein Suchfenster an.

3. Suchen Sie die Admin-Aufgabe, die die Benutzersynchronisierung auslöst, und wählen Sie sie aus.

4. Wählen Sie für die Aufgabe auf der Registerkarte "Profil" eine der folgenden Optionen im Feld "Benutzersynchronisierung" aus:

   - **Deaktiviert**: Diese Aufgabe löst keine Benutzersynchronisierung aus.
   - **Bei Abschluss der Aufgabe**: CA IdentityMinder startet den Benutzersynchronisierungsdurchlauf nach Abschluss aller Ereignisse. Diese Einstellung ist die Standardsynchronisierungsoption für die Aufgaben "Benutzer erstellen", "Benutzer ändern" und "Benutzer löschen". Die Standardeinstellung für alle anderen Aufgaben lautet "Deaktiviert".

     Hinweis: Beim Aktivieren der Option "Bei Abschluss der Aufgabe" für eine Aufgabe, die mehrere Ereignisse einschließt, synchronisiert CA IdentityMinder die Benutzer erst dann, wenn alle Ereignisse in der Aufgabe abgeschlossen sind. Falls für eines oder mehrere Ereignisse die Genehmigung des Workflows erforderlich ist, kann dieser Prozess mehrere Tage dauern. Um zu vermeiden, dass CA IdentityMinder mit der Anwendung der Identitätsrichtlinien wartet, bis alle Ereignisse abgeschlossen sind, wählen Sie die Option "Bei jedem Ereignis" aus.
   - **Bei jedem Ereignis**: CA IdentityMinder startet den Benutzersynchronisierungsdurchlauf, wenn das jeweilige Ereignis in einer Aufgabe abgeschlossen ist.

     Bei Aufgaben mit einem primären und einem sekundären Ereignis für denselben Benutzer kann das Einstellen der Benutzersynchronisierung auf die Option "Bei jedem Ereignis" zu mehr Auswertungen führen, für die Richtlinien für einen Benutzer gelten, als wenn die Option "Bei Abschluss der Aufgabe" ausgewählt wird.

Manuelles Synchronisieren von Benutzern

Möglicherweise möchten Sie einen Benutzer manuell mit einem Identitätsrichtliniensatz synchronisieren, um sicherzustellen, dass ein bestimmtes Benutzerkonto die richtigen Berechtigungen besitzt oder eine Konformitätsrichtlinie erfüllt.

Sie können einen Benutzer manuell mit Hilfe der Aufgabe "Benutzer synchronisieren" in der Benutzerkonsole von CA IdentityMinder synchronisieren.

Hinweis: Damit die Aufgabe "Benutzer synchronisieren" ordnungsgemäß funktioniert, muss die Option "Benutzersynchronisierung" auf "Deaktiviert" eingestellt sein, und die Option "Kontosynchronisierung" muss auf "Bei Abschluss der Aufgabe" oder "Bei jedem Ereignis" eingestellt sein. Wählen Sie für eine bessere Leistung die Option "Bei Abschluss der Aufgabe" aus. Diese Optionen werden auf der Registerkarte "Profil" für die Aufgabe "Benutzer synchronisieren" gesetzt.

Die Aufgabe "Benutzer synchronisieren" weist folgende Registerkarten auf:

- **Aktuell erfüllte Richtlinien**: Zeigt eine Liste mit Identitätsrichtlinien an, die CA IdentityMinder für den Benutzer übernimmt, wenn die Aufgabe "Benutzer synchronisieren" gesendet wird.

  Hinweis: Die Registerkarte "Derzeit erfüllte Richtlinien" zeigt nur die Identitätsrichtlinien an, die zum Zeitpunkt des Zugriffs auf die Aufgabe "Benutzer synchronisieren" für den Benutzer gelten. Wenn der Benutzer mit diesen Richtlinien synchronisiert wird, können Änderungen auftreten, die weitere Identitätsrichtlinien auslösen. Um CA IdentityMinder daran zu hindern, die neuen Richtlinien zu übernehmen, bevor Sie sie überprüft haben, stellen Sie die Rekursionsebene für Identitätsrichtliniensätze in der Management-Konsole von CA IdentityMinder auf 1. Greifen Sie nach dem Senden der Aufgabe "Benutzer synchronisieren" erneut darauf zu, um die Richtlinien zu überprüfen.

- **Bereits übernommene Richtlinien**: Zeigt eine Liste mit Identitätsrichtlinien an, die bereits für den Benutzer übernommen worden sind.

- **Synchronisierungszusammenfassung**: Zeigt alle Identitätsrichtlinien an, die für den Benutzer gelten, und die Änderungsaktivitäten für diese Richtlinien.

So synchronisieren Sie ein Benutzerkonto:

1. Melden Sie sich bei Identity Manager als Benutzer an, der die Aufgaben "Benutzer synchronisieren" verwenden kann. (Standardmäßig können Benutzer mit der Rolle "System-Manager" diese Aufgabe verwenden.)
2. Wählen Sie zunächst die Option "Richtlinien auswählen" und dann die Option "Benutzer synchronisieren" aus.

   Die Aufgabe "Benutzer synchronisieren" öffnet sich.
3. Wählen Sie die Registerkarte "Synchronisierungszusammenfassung" aus.
4. Überprüfen Sie die Richtlinien und die damit verknüpften Aktionen, die CA IdentityMinder für den Benutzer übernimmt, und klicken Sie dann auf "Senden".

Verifizieren der Benutzersynchronisierung

Um zu verifizieren, dass die entsprechenden Änderungen stattfinden, wenn ein Benutzer mit Identitätsrichtlinien synchronisiert wird, prüfen Sie in der Aufgabe "Benutzer synchronisieren" die Registerkarte "Bereits übernommene Richtlinien".

1. Melden Sie sich bei CA IdentityMinder als Benutzer an, der die Aufgabe "Benutzer synchronisieren" verwenden kann. (Standardmäßig können Benutzer mit der Rolle "System-Manager" diese Aufgabe verwenden.)
2. Wählen Sie zunächst die Option "Richtlinien auswählen" und dann die Option "Benutzer synchronisieren" aus.

   Die Aufgabe "Benutzer synchronisieren" öffnet sich.

3. Wählen Sie die Registerkarte "Bereits übernommene Richtlinien" aus.
4. Überprüfen Sie die Richtlinien und die mit ihnen verknüpften Aktionen, die CA IdentityMinder für den Benutzer übernommen hat.

Identitätsrichtliniensätze in einer Identity Manager-Umgebung

Die folgenden Abschnitte beschreiben unterschiedliche Möglichkeiten, Identitätsrichtlinien zu verwenden:

- Beispiel: Automatisches Füllen von Benutzerattributen (siehe Seite 492)
- Beispiel: Zuweisen von Ressourcen und Berechtigungen (siehe Seite 493)
- Beispiel: Durchsetzen von Konformität (siehe Seite 494)
- Beispiel: Durchsetzen der Trennung von Pflichten (siehe Seite 495)

Beispiel: Automatisches Füllen von Benutzerattributen

Sie können einen Identitätsrichtliniensatz verwenden, um Benutzerattributwerte basierend auf einem weiteren Attributwert oder einer Benutzerberechtigung automatisch zuzuweisen. Sie können z. B. einen Identitätsrichtliniensatz erstellen, der basierend auf dem Home Office des Benutzers eine Postanschrift des Benutzers automatisch ausfüllt.

Um einen Identitätsrichtliniensatz für Arbeitnehmeradressen zu konfigurieren, erstellen Sie eine Identitätsrichtlinie mit den folgenden Einstellungen für jeden Bürostandort:

Einstellung	Wert
Richtlinienbedingung	Büro = <Büro_Standort>
Aktion zu "Richtlinie anwenden"	geben Sie eine Straße = <beliebige Straße> an geben Sie eine Stadt = <beliebige Stadt> an geben Sie ein Bundesland/einen Kanton = <beliebiges Bundesland oder beliebiger Kanton> an Geben Sie eine Postleitzahl = <beliebige Postleitzahl> an

Die folgende Abbildung stellt Beispielrichtlinien in dem Identitätsrichtliniensatz "Arbeitnehmeradressen" dar.

Identitätsrichtlinien

Richtliniensatz

	Richtlinienname	Richtlinien-Mitgliedsregel	Aktion zu "Richtlinie anwenden"
	Boston	wobei: (Office = "Boston")	Addresses auf 201 Road festlegen City auf Boston festlegen State / Province auf MA festlegen Postal Code auf 10021 festlegen
	NY	wobei: (Office = "NY")	Addresses auf 105 5th festlegen City auf NY festlegen State / Province auf NY festlegen Postal Code auf 10017 festlegen

Beispiel: Zuweisen von Ressourcen und Berechtigungen

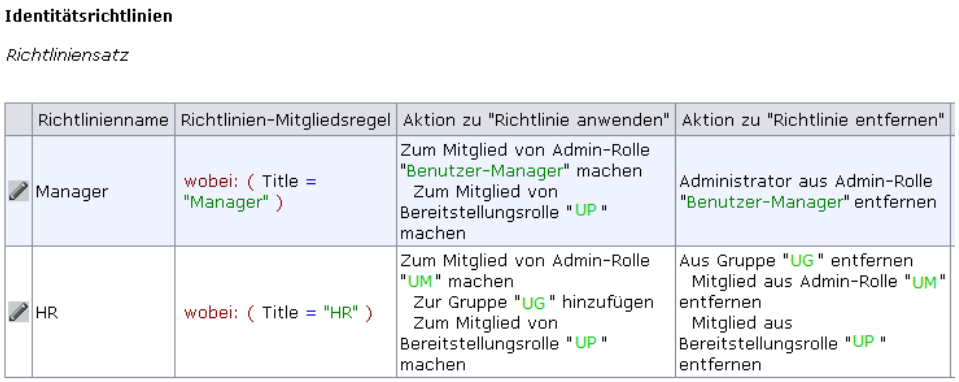
Identitätsrichtlinien können automatisch Ressourcen wie z. B. Domänenkonten zuweisen oder Berechtigungen gewähren, wie z. B. einen Benutzer als Mitglied einer Rolle aufzunehmen, wenn Benutzer die Richtlinienbedingung erfüllen. Sie können z. B. einen Satz Identitätsrichtlinien erstellen, die Ressourcen und Rollen basierend auf dem Titel eines Benutzers zuweisen.

Um einen Identitätsrichtliniensatz zum Zuweisen von Ressourcen und Rollen zu erstellen, erstellen Sie eine Identitätsrichtlinie mit den folgenden Einstellungen für jeden Titel in Ihrer Organisation:

Einstellung	Wert
Richtlinienbedingung	Titel = <beliebiger_Titel>
Aktion zu "Richtlinie anwenden"	Alle Aktionen, die Ressourcen oder Berechtigungen Benutzern zuweisen, die die Richtlinienbedingung erfüllen, z. B.: ■ Zum Mitglied von <beliebige_Gruppe> machen ■ Zum Mitglied von Admin-Rolle <beliebige_Admin_Rolle> machen ■ Zum Mitglied von Bereitstellungsrolle <beliebige_Bereitstellungsrolle> machen

Einstellung	Wert
Aktion zu "Richtlinie entfernen"	Alle Aktionen, die Ressourcen oder Berechtigungen entfernen, wenn ein Benutzer die Richtlinienbedingung nicht mehr erfüllt. Wenn Identity Manager den Benutzer z. B. zu einem Mitglied einer Rolle gemacht hat, als die Identitätsrichtlinie übernommen wurde, möchten Sie Identity Manager möglicherweise so konfigurieren, dass er die Rolle widerruft, wenn der Benutzer die Richtlinienbedingung nicht mehr erfüllt.

Die folgende Abbildung stellt Beispielrichtlinien im Identitätsrichtliniensatz "Arbeitnehmerressourcen" dar.



Identitätsrichtlinien

Richtliniensatz

	Richtlinienname	Richtlinien-Mitgliedsregel	Aktion zu "Richtlinie anwenden"	Aktion zu "Richtlinie entfernen"
	Manager	wobei: (Title = "Manager")	Zum Mitglied von Admin-Rolle "Benutzer-Manager" machen Zum Mitglied von Bereitstellungsrolle "UP" machen	Administrator aus Admin-Rolle "Benutzer-Manager" entfernen
	HR	wobei: (Title = "HR")	Zum Mitglied von Admin-Rolle "UM" machen Zur Gruppe "UG" hinzufügen Zum Mitglied von Bereitstellungsrolle "UP" machen	Aus Gruppe "UG" entfernen Mitglied aus Admin-Rolle "UM" entfernen Mitglied aus Bereitstellungsrolle "UP" entfernen

Beispiel: Durchsetzen von Konformität

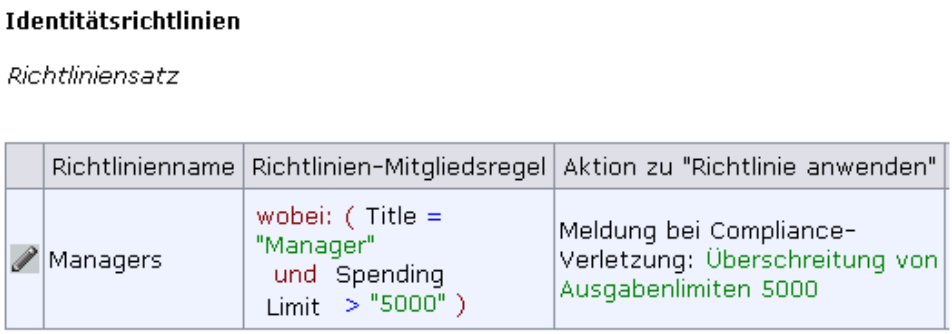
Sie können Identitätsrichtlinien konfigurieren, um Bedingungen zu definieren, die vorhanden sein müssen oder nicht vorhanden sein dürfen, und um bestimmte Aktionen basierend auf der Auswertung dieser Bedingungen auszuführen. Sie können z. B. eine Konformitätsrichtlinie definieren, die festlegt, dass für Manager eine Ausgabenbeschränkung von $ 5.000 gelten muss. Wenn für einen Manager eine Ausgabenbeschränkung von $ 10.000 gilt, kann CA IdentityMinder die Ausgabenbeschränkung des Managers zurücksetzen und eine Konformitätsverletzung für Audit-Zwecke aufzeichnen.

Um einen Konformitätsrichtliniensatz zum Durchsetzen von Ausgabenbeschränkungen zu erstellen, erstellen Sie eine Identitätsrichtlinie mit den folgenden Einstellungen:

Einstellung	Wert
Einmal übernehmen	Nicht aktiviert
Konformität	Aktiviert

Einstellung	Wert
Richtlinienbedingung	Alle Bedingungen, die Konformität oder eine Konformitätsverletzung definieren. Beispiel: Titel=<beliebiger_Titel> UND Ausgabenbeschränkung > <beliebige Ausgabenbeschränkung>
Aktion zu "Richtlinie anwenden"	Die Aktionen, die CA IdentityMinder ausführen soll, wenn die Richtlinienbedingung zutrifft. Beispiel: ■ Meldung bei Konformitätsverletzung: Ausgabenbeschränkung überschritten ■ Ausgabenbeschränkung auf <beliebiger_Wert> festlegen

Die folgende Abbildung stellt die in diesem Beispiel beschriebene Beispielkonformitätsrichtlinie dar.



Beispiel: Durchsetzen der Trennung von Pflichten

Identitätsrichtlinien können Rollen definieren, die sich gegenseitig ausschließen und einem Benutzer nicht gleichzeitig gewährt werden können. Sie können z. B. verhindern, dass ein Benutzer-Manager, der Gehaltserhöhungen gewähren kann, auch ein Gehaltsgenehmiger ist.

Um einen Identitätsrichtliniensatz zu erstellen, der die Trennung von Pflichten durchsetzt, erstellen Sie eine Identitätsrichtlinie mit den folgenden Einstellungen:

Einstellung	Wert
Einmal übernehmen	Nicht aktiviert
Konformität	Aktiviert

Einstellung	Wert
Richtlinienbedingung	Verwenden Sie die Option "in <administrative-Schnittmengen-Beschränkung>", um einen Satz von Bedingungen zu definieren, die eine Geschäftsregel verletzen. Wenn ein Benutzer alle Bedingungen erfüllt, führt Identity Manager die Aktionen in dem Feld "Aktion zu Richtlinie übernehmen" aus. Stellen Sie z. B. die Richtlinienbedingung folgendermaßen ein: Schnittmenge (Wer ist Mitglied von <beliebige_Rolle>), und wer ist Mitglied von <beliebige_andere_Rolle>)
Aktion zu "Richtlinie anwenden"	Die Aktionen, die Identity Manager ausführen soll, wenn die Richtlinienbedingung zutrifft. Beispiel: ■ Meldung bei Konformitätsverletzung: Benutzer verfügt über Rollen, die sich gegenseitig ausschließen ■ Mitglied aus <beliebige_Rolle> entfernen

Die folgende Abbildung stellt die Identitätsrichtlinie in diesem Beispiel dar.

Identitätsrichtlinien

Richtliniensatz

	Richtlinienname	Richtlinien-Mitgliedsregel	Aktion zu "Richtlinie anwenden"
	Einschränkung	Schnittmenge (als Mitglieder von (Admin-Rolle "Benutzer-Manager") und als Mitglieder von (Admin-Rolle "Genehmiger für Benutzer"))	Meldung bei Compliance-Verletzung: Benutzer hat sich gegenseitig ausschließenden Mitglied aus Admin-Rolle "Genehmiger für Benutzer" entfernen

Präventive Identitätsrichtlinien

Eine *präventive Identitätsrichtlinie* ist ein Typ von Identitätsrichtlinie, der verhindert, dass Benutzer Berechtigungen erhalten, die zu Interessenkonflikten oder Betrug führen können. Diese Richtlinien unterstützen die Anforderungen eines Unternehmens hinsichtlich der Trennung von Pflichten (Segregation of Duties, SOD).

Präventive Identitätsrichtlinien werden vor dem Senden einer Aufgabe ausgeführt. Mit ihnen kann ein Administrator nach Richtlinienverletzungen suchen, bevor er Berechtigungen zuweist oder Profilattribute ändert. Wenn eine Verletzung vorliegt, kann sie der Administrator beheben, bevor er die Aufgabe sendet.

Beispielsweise kann ein Unternehmen eine präventive Identitätsrichtlinie erstellen, die nicht zulässt, dass Benutzer, die die Rolle "Benutzer-Manager" besitzen, auch die Rolle "Genehmiger für Benutzer" besitzen. Wenn ein Administrator die Aufgabe "Benutzer ändern" verwendet, um einem Benutzer-Manager die Rolle "Genehmiger für Benutzer" zu geben, zeigt CA IdentityMinder eine Meldung über die Verletzung an. Der Administrator kann die Rollenzuweisungen ändern, um die Verletzung zu beheben, bevor er die Aufgabe sendet.

Sie können präventive Identitätsrichtlinien für die folgenden Änderungen erstellen:

- **Rollenmitgliedschaft**

  Verhindert, dass Benutzer bestimmte Rollen gleichzeitig besitzen.

  Beispielsweise können Benutzer nicht zur gleichen Zeit die Rollen "Benutzer-Manager" und "Genehmiger für Benutzer" besitzen.

- **Rollenadministratoren**

  Verhindert, dass Benutzer Administratoren bestimmter Rollen sind, wenn sie Administratoren anderer Rollen sind.

  Beispielsweise können Benutzer nicht zur gleichen Zeit Administratoren für die Rollen "Benutzer-Manager" und "Genehmiger für Benutzer" sein.

- **Benutzerattribute**

  Verhindert, dass Benutzer bestimmte Profilattribute gleichzeitig besitzen.

  Beispielsweise können Benutzer nicht den Titel "Senior Account" haben und zur IT-Abteilung gehören.

- **Organisationsattribute**

  Verhindert, dass Benutzerprofile in einer bestimmten Organisation erstellt werden.

  Beispielsweise können Administratoren keine Mitarbeiterprofile in der Organisation "Lieferanten" erstellen.

- **Gruppenattribute**

  Verhindert die Mitgliedschaft von Benutzern in bestimmten Gruppen.

  Beispielsweise können Benutzer nicht Mitglied der Gruppe "Projektteam" und der Gruppe "Accounting" sein.

Weitere Informationen:

Aktionen für Verletzungen präventiver Identitätsrichtlinien (siehe Seite 498)

Aktionen für Verletzungen präventiver Identitätsrichtlinien

Wenn eine präventive Identitätsrichtlinie für eine geschäftliche Änderung gilt, führt CA als Reaktion auf die Verletzung bestimmte Aktionen aus.

Wenn Sie eine dieser Aktionen in einer Identitätsrichtlinie angeben, legen Sie eine Meldung fest, die die Verletzung beschreibt. Diese Meldung wird in der Audit-Datenbank aufgezeichnet. Abhängig vom Typ der Aktion kann die Meldung den Benutzern auch in der Benutzerkonsole angezeigt und in "Gesendete Aufgaben anzeigen" aufgezeichnet werden.

Sie können für eine präventive Identitätsrichtlinie die folgenden Aktionen konfigurieren:

Akzeptieren

CA IdentityMinder zeigt in "Gesendete Aufgaben anzeigen" eine Meldung mit einer Beschreibung der Verletzung an, lässt jedoch das Senden der Aufgabe zu.

Ablehnen

CA IdentityMinder zeigt in der Benutzerkonsole eine Meldung an und verhindert das Senden der Aufgabe.

Warnung

CA IdentityMinder zeigt in der Benutzerkonsole und in "Gesendete Aufgaben anzeigen" eine Meldung an. Diese Aktion kann optional einen Workflow-Prozess auslösen, der eine Genehmigung eines entsprechenden Benutzers erfordert, bevor CA IdentityMinder die Aufgabe ausführt.

Um einen Workflow-Prozess auszulösen, ordnen Sie in Aufgaben, die die Verletzung verursachen können, die präventive Identitätsrichtlinie einem richtlinienbasierten Workflow-Prozess zu (siehe Seite 505).

Wenn die Verletzung beispielsweise auftritt, wenn ein Benutzer bestimmte Rollen gleichzeitig erhält, konfigurieren Sie den Workflow-Prozess für alle Aufgaben, die Benutzern diese Rollen zuweisen.

Hinweis: Wenn Sie den richtlinienbasierten Workflow-Prozess für die Aufgabe konfigurieren, muss die Genehmigungsregel den Namen der präventiven Identitätsrichtlinie referenzieren.

Funktionsweise von präventiven Identitätsrichtlinien

Der folgende Beispielprozess verdeutlicht die Funktionsweise von präventiven Identitätsrichtlinien:

1. Ein Identitätsrichtlinienadministrator erstellt eine präventive Identitätsrichtlinie, die nicht zulässt, dass Benutzer mit dem Titel "Senior Accountant" in der IT-Abteilung sind.

   Bei der Definition dieser Identitätsrichtlinie legt der Administrator fest, dass CA IdentityMinder alle Änderungen ablehnen soll, die diese Richtlinie verletzen.

2. Ein Personalleiter verwendet die Aufgabe "Benutzer erstellen", um ein Benutzerprofil für einen neuen Senior Accountant zu erstellen. Der Personalleiter wählt den Titel des Benutzers korrekt aus, er wählt jedoch versehentlich die IT-Abteilung aus.

3. Der Personalleiter füllt die übrigen Felder in der Aufgabe "Benutzer erstellen" aus und klickt auf "Senden".

4. CA IdentityMinder erkennt, dass die Aufgabe Änderungen beinhaltet, die in einer Identitätsrichtlinie definiert sind, und wertet die Änderungen in Bezug auf Verletzungen aus.

5. CA IdentityMinder erkennt die Verletzung, zeigt dem Personalleiter eine Meldung an und verhindert das Senden der Aufgabe.

   Außerdem zeichnet CA IdentityMinder die Meldung in der Audit-Datenbank auf.

6. Der Personalleiter liest in der Meldung die Details zu der Verletzung und ändert die Abteilung des Benutzers in "Finanzen". Anschließend sendet der Administrator die Aufgabe erneut.

7. CA IdentityMinder wertet die vorgeschlagenen Änderungen anhand aller anwendbaren Identitätsrichtlinien aus und lässt anschließend das Senden der Aufgabe "Benutzer erstellen" zu.

Wichtige Hinweise zu präventiven Identitätsrichtlinien

Beachten Sie vor der Implementierung von präventiven Identitätsrichtlinien Folgendes:

- Präventive Identitätsrichtlinien verhindern nur solche Verletzungen, die aufgrund von vorgeschlagenen Änderungen in der aktuellen Aufgabe auftreten würden. Sie verhindern keine bereits bestehenden Verletzungen.

  Beispielsweise erstellt ein Unternehmen eine präventive Identitätsrichtlinie, die nicht zulässt, dass Benutzer gleichzeitig die Rollen "Benutzer-Manager" und "Genehmiger für Benutzer" besitzen. Ein Administrator weist einem Benutzer, der bereits die Rollen "Benutzer-Manager" und "Genehmiger für Benutzer" besitzt, die Rolle "Gruppen-Manager" zu. CA IdentityMinder lässt die erfolgreiche Durchführung der neuen Zuweisung zu, da diese Änderung keine direkte Verletzung der Richtlinie verursacht.

- Wenn mehrere präventive Identitätsrichtlinien für eine Reihe von vorgeschlagenen Änderungen gelten, wendet CA IdentityMinder zuerst die Richtlinien mit Ablehnungsaktionen an.

- Geben Sie in den Bedingungen für präventive Identitätsrichtlinien keine dynamischen Gruppen an. (Richtlinienbedingungen legen die Gruppe der Benutzer fest, für die die präventive Identitätsrichtlinie gilt.)

  Beispielsweise hat ein Unternehmen eine dynamische Gruppe, die alle Benutzer mit dem Titel "Manager" enthält. Das Unternehmen erstellt außerdem eine präventive Identitätsrichtlinie, die verhindert, dass Mitglieder der Gruppe "Manager" die Rolle "Auftragnehmer" besitzen.

  Ein Administrator ändert den Titel eines Benutzers, der die Rolle "Auftragnehmer" besitzt, in "Manager". Durch diese Änderung wird der Benutzer Mitglied der Gruppe "Manager", *nachdem* die Aufgabe erfolgreich gesendet wurde. Der Titel des Benutzers lautet jedoch zum Zeitpunkt der Richtlinienauswertung durch CA IdentityMinder nicht "Manager", daher wird keine Verletzung erkannt.

- Der Rolleneigentümerfilter und der LDAP-Abfragefilter werden bei Richtlinienbedingungen für präventive Identitätsrichtlinien nicht unterstützt.

Erstellen einer präventiven Identitätsrichtlinie

Bevor Sie eine präventive Identitätsrichtlinie erstellen, erstellen Sie einen Identitätsrichtliniensatz, der mehrere Identitätsrichtlinien logisch gruppiert.

Hinweis: Bevor Sie beginnen, lesen Sie Wichtige Hinweise zu präventiven Identitätsrichtlinien (siehe Seite 500).

So erstellen Sie einen Identitätsrichtliniensatz für eine präventive Identitätsrichtlinie:

1. Öffnen Sie in der Benutzerkonsole "Richtlinien", "Identitätsrichtliniensatz erstellen".

   Erstellen Sie einen neuen Identitätsrichtliniensatz, oder verwenden Sie einen vorhandenen Identitätsrichtliniensatz als Vorlage.

2. Definieren Sie das Profil für den Identitätsrichtliniensatz (siehe Seite 476) auf der Registerkarte "Profil".

3. Erstellen Sie eine Richtliniensatz-Mitgliedsregel (siehe Seite 477) auf der Registerkarte "Richtlinien".

4. Erstellen Sie wie folgt eine präventive Identitätsrichtlinie:

   a. Klicken Sie auf "Hinzufügen".

   b. Geben Sie einen Namen für die Identitätsrichtlinie ein.

      Hinweis: Die Einstellungen "Einmal übernehmen" und "Konformität" gelten nicht für präventive Identitätsrichtlinien.

   c. Identifizieren Sie die Benutzer, für die die Richtlinie gilt, im Abschnitt "Richtlinienbedingung".

      Hinweis: Der Rolleneigentümerfilter und der LDAP-Abfragefilter werden für präventive Identitätsrichtlinien nicht unterstützt.

d. Definieren Sie im Feld "Aktion zu Richtlinie anwenden" die Aktionen, die CA IdentityMinder ausführt, wenn CA IdentityMinder eine Richtlinienverletzung erkennt:

Akzeptieren

CA IdentityMinder zeigt in "Gesendete Aufgaben anzeigen" eine Meldung mit einer Beschreibung der Verletzung an, lässt jedoch das Senden der Aufgabe zu.

Ablehnen

CA IdentityMinder zeigt in der Benutzerkonsole eine Meldung an und verhindert das Senden der Aufgabe.

Warnung

CA IdentityMinder zeigt in der Benutzerkonsole und in "Gesendete Aufgaben anzeigen" eine Meldung an. Diese Aktion kann optional einen Workflow-Prozess auslösen (siehe Seite 503).

Wenn Sie eine dieser Aktionen auswählen, zeigt CA IdentityMinder ein Textfeld an, in dem Sie die Meldung angeben können, die bei einer Verletzung angezeigt wird.

e. Geben Sie die Meldung im Textfeld an.

Hinweis: Wenn Sie die Benutzerkonsole lokalisieren, können Sie im Meldungsfeld anstelle von Text einen Ressourcenschlüssel angeben. Im *User Console Design Guide* finden Sie weitere Informationen zu Ressourcenschlüsseln.

f. Fügen Sie bei Bedarf zusätzliche Aktionen hinzu, und klicken Sie auf "OK".

5. Geben Sie die Eigentümer für den Identitätsrichtliniensatz an (siehe Seite 487)

Hinweis: Stellen Sie vor der Verwendung des von Ihnen erstellten Identitätsrichtliniensatzes sicher, dass Identitätsrichtlinien in der Managementkonsole aktiviert sind. Weitere Informationen finden Sie im *Konfigurationshandbuch.*

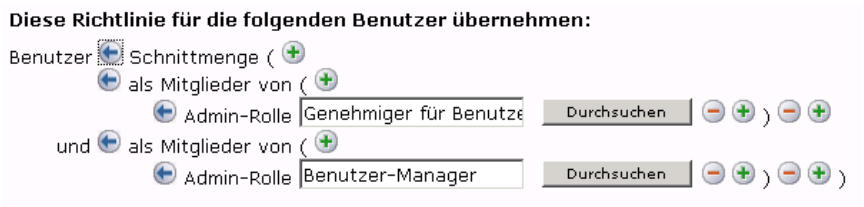
Anwendungsfall: Verhindern, dass Benutzer widersprüchliche Rollen besitzen

Forward, Inc. möchte verhindern, dass seine Mitarbeiter gleichzeitig die Rollen "Benutzer-Manager" und "Genehmiger für Benutzer" besitzen. Mitarbeiter, die beide Rollen besitzen, können Benutzerattribute, wie z. B. das Gehalt, ändern und unberechtigerweise genehmigen.

Um diese Situation zu verhindern, erstellt Forward, Inc. eine präventive Identitätsrichtlinie, die für Benutzer gilt, die die Rollen "Benutzer-Manager" und "Genehmiger für Benutzer" besitzen. Wenn ein Administrator versucht, einem Benutzer diese Rollen zu geben, lehnt CA IdentityMinder das Senden der Aufgabe ab und zeigt eine Meldung mit einer Erklärung zu der Verletzung an.

Sie konfigurieren eine präventive Identitätsrichtlinie zur Unterstützung dieses Anwendungsfalls wie folgt:

- Erstellen Sie einen Identitätsrichtliniensatz für die Richtlinie, die Sie erstellen möchten.
- Erstellen Sie eine präventive Identitätsrichtlinie mit den folgenden Einstellungen:
  - Richtlinienbedingung:



  - Aktion zu "Richtlinie anwenden":
    - Ablehnen mit der Nachricht: Der Benutzer kann nicht Mitglied der Rollen "Genehmiger für Benutzer" und "Benutzer-Manager" sein

Workflow und präventive Identitätsrichtlinien

Wenn eine präventive Identitätsrichtlinie für die Ausgabe einer Warnung konfiguriert ist, können Sie für Aufgaben, die möglicherweise eine Verletzung auslösen, einen richtlinienbasierten Workflow-Prozess auf Aufgabenebene definieren, der der Identitätsrichtlinie zugeordnet wird. Wenn beispielsweise eine Identitätsrichtlinie verhindert, dass Senior Accountants Mitglieder der IT-Abteilung sind, definieren Sie einen richtlinienbasierten Workflow-Prozess auf Aufgabenebene für die Aufgaben "Benutzer erstellen" und "Benutzer ändern".

Alle Arbeitselemente, die als Ergebnis eines richtlinienbasierten Workflows auf Aufgabenebene generiert werden, müssen genehmigt werden, bevor CA IdentityMinder die Aufgabe ausführt. Genehmigern wird ein Arbeitslistenelement angezeigt, wenn sie sich bei der Benutzerkonsole anmelden. Wenn der Genehmiger auf das Arbeitslistenelement klickt, wird eine Genehmigungsaufgabe angezeigt, die die Warnmeldung mit der Beschreibung der Verletzung enthält. Der Genehmiger kann die Aufgabe basierend auf der Verletzung genehmigen oder ablehnen.

Richtlinienbasierte Workflow-Prozesse werden präventiven Identitätsrichtlinien anhand des Richtliniennamens zugeordnet.

Weitere Informationen:

Richtlinienbasierter Workflow (siehe Seite 340)

Verletzungen von Identitätsrichtlinien in Genehmigungsaufgaben

Wenn eine präventive Identitätsrichtlinie einem Workflow-Prozess für eine Aufgabe zugeordnet wird, generiert CA IdentityMinder ein Arbeitslistenelement für die entsprechenden Genehmiger. Diese Genehmiger verwenden eine Genehmigungsaufgabe, um die Änderung, die die Richtlinienverletzung ausgelöst hat, zu genehmigen oder abzulehnen.

Die standardmäßige Genehmigungsaufgabe enthält einen Abschnitt, in dem Verletzungen der Identitätsrichtlinie aufgelistet sind. Wenn die vorgeschlagenen Änderungen mehrere präventive Identitätsrichtlinien auslösen, können mehrere Verletzungen vorhanden sein.

Jede Verletzung kann einen der folgenden Status besitzen:

- **Auswertung steht aus**

  CA IdentityMinder hat noch nicht mit der Auswertung der Genehmigungsregeln für die Aufgabe begonnen. Dies ist der anfängliche Status.

- **Genehmigung erwarten**

  CA IdentityMinder hat eine Übereinstimmung für die in den Genehmigungsregeln definierte Identitätsrichtlinie gefunden und den zugeordneten Workflow-Prozess ausgelöst.

- **Bestätigt**

  Ein Genehmiger hat die vorgeschlagenen Änderungen genehmigt. CA IdentityMinder nimmt die Änderungen vor, die die Verletzungen der präventiven Identitätsrichtlinie ausgelöst haben.

- **Abgelehnt**

  Ein Genehmiger hat die vorgeschlagene Änderung abgelehnt. Die Aufgabe wird zurückgewiesen.

- **Kein Workflow konfiguriert**

  Für diese Verletzung wurde kein Workflow-Prozess konfiguriert. Die Aufgabe wird ausgeführt, ohne dass eine Genehmigung erforderlich ist.

Konfigurieren des Workflows für präventive Identitätsrichtlinien

Sie konfigurieren den Workflow für präventive Identitätsrichtlinien in den Admin-Aufgaben, die Änderungen enthalten, die eine Identitätsrichtlinienverletzung auslösen können.

Wenn die präventive Identitätsrichtlinie beispielsweise verhindert, dass Benutzer bestimmte Admin-Rollen zur gleichen Zeit besitzen, konfigurieren Sie Aufgaben, die Admin-Rollen zuweisen, um den Workflow für präventive Identitätsrichtlinien zu unterstützen.

Hinweis: Erstellen Sie vor dem Konfigurieren des Workflows eine präventive Identitätsrichtlinie mit den folgenden Einstellungen:

- Ein eindeutiger Richtlinienname

  Der Richtlinienname muss in allen Identitätsrichtliniensätzen eindeutig sein, da Workflow-Prozesse präventiven Identitätsrichtlinien anhand des Richtliniennamens zugeordnet werden.

  Wenn mehrere präventive Identitätsrichtlinien denselben Namen besitzen, können mehrere Workflow-Prozesse gelten.

- Warnung im Feld "Aktion zu Richtlinie anwenden"

  "Warnung" ist die einzige Aktion, die einen Workflow-Prozess auslösen kann.

Legen Sie nach dem Konfigurieren der präventiven Identitätsrichtlinie die Aufgaben fest, die die Richtlinienverletzung auslösen können. Erstellen Sie anschließend eine Workflow-Genehmigungsrichtlinie (siehe Seite 506) für diese Aufgaben.

Erstellen einer Workflow-Genehmigungsrichtlinie für präventive Identitätsrichtlinien

Sie können für eine Admin-Aufgabe einen richtlinienbasierten Workflow-Prozess auf Aufgabenebene konfigurieren. Dieser Workflow-Prozess umfasst eine oder mehrere Genehmigungsrichtlinien, die eine präventive Identitätsrichtlinie mit einem Workflow verknüpfen können. CA IdentityMinder führt den Workflow aus, wenn eine Verletzung der zugeordneten präventiven Identitätsrichtlinie auftritt.

Hinweis: Weitere Informationen zu richtlinienbasierten Workflow-Prozessen auf Aufgabenebene finden Sie unter Richtlinienbasierter Workflow (siehe Seite 340).

So erstellen Sie eine Workflow-Genehmigungsrichtlinie für präventive Identitätsrichtlinien:

1. Ändern Sie die Admin-Aufgaben, die Änderungen zulassen, die eine Verletzung einer präventiven Identitätsrichtlinie auslösen können.

   Wenn beispielsweise eine Identitätsrichtlinienverletzung auftritt, weil ein Benutzer die Rollen "Benutzer-Manager" und "Genehmiger für Benutzer" besitzt, ändern Sie die Admin-Aufgaben, die Administratoren das Zuweisen von Rollen ermöglichen, z. B. "Benutzer erstellen", "Benutzer ändern" und "Mitglieder/Administratoren von Admin-Rolle ändern".

2. Klicken Sie auf das Symbol "Bearbeiten" neben dem Feld "Workflow-Prozess" auf der Registerkarte "Profil" für die Aufgabe, um einen Workflow-Prozess hinzuzufügen.

   CA IdentityMinder zeigt das Fenster "Workflow-Konfiguration der Aufgabenebenen" an.

3. Wählen Sie "Richtlinien-basierend", und klicken Sie anschließend auf "Hinzufügen".

4. Wählen Sie im Abschnitt "Genehmigungsregel" das Objekt "Verletzung der Identitätsrichtlinie" aus.

5. Wählen Sie im Feld "Identitätsrichtlinie" einen Filter aus, der festlegt, welche Identitätsrichtlinien den mit der Genehmigungsrichtlinie verknüpften Workflow auslösen.

   Fügen Sie den Namen der Identitätsrichtlinie, *nicht* den Namen des Identitätsrichtliniensatzes, zum Filter hinzu.

6. Konfigurieren Sie die Felder "Regelauswertung", "Richtlinienreihenfolge" und "Richtlinienbeschreibung" wie erforderlich.

7. Wählen Sie einen Workflow-Prozess aus, und klicken Sie anschließend auf "OK".

   Wenn Sie einen Workflow-Prozess auswählen, zeigt CA IdentityMinder zusätzliche Felder an.

8. Geben Sie nach Bedarf Genehmigungsaufgaben und Genehmiger an.

   CA IdentityMinder ordnet den Workflow-Prozess der präventiven Identitätsrichtlinie zu.

Anwendungsfall: Genehmigen von Titeln

Eine Unternehmensrichtlinie von Forward, Inc. besagt, dass alle Manager Vollzeitmitarbeiter sein müssen. Forward, Inc. hat jedoch in letzter Zeit viele Auftragnehmer für spezielle Projekte eingestellt. Um diese speziellen Projekte effizient durchzuführen, erhalten einige Auftragnehmer den Titel "Manager". Forward, Inc. möchte, dass Genehmigungen vom Leiter der Personalabteilung erforderlich sind, bevor Administratoren einem Auftragnehmer den Titel "Manager" zuweisen können.

Um den Genehmigungsprozess in diesen Situationen zu automatisieren, erstellt Forward, Inc. eine präventive Identitätsrichtlinie mit dem Namen "Manager-Titel für Auftragnehmer", die erkennt, wenn der Titel eines Benutzers "Manager" und die Organisation eines Benutzers "Auftragnehmer" ist. Forward, Inc. konfiguriert darüber hinaus einen richtlinienbasierten Genehmigungsprozess für die Aufgabe "Benutzer ändern". Dieser Genehmigungsprozess wird ausgelöst, wenn die Richtlinie "Manager-Titel für Auftragnehmer" verletzt wird.

Wenn ein Administrator den Titel eines Auftragnehmers in "Manager" ändert, zeigt CA IdentityMinder eine Warnmeldung an und sendet ein Arbeitselement zur Genehmigung an den Leiter der Personalabteilung. CA IdentityMinder ändert den Titel des Auftragnehmers erst, wenn das Arbeitselement genehmigt wurde.

Um Unterstützung für diesen Anwendungsfall zu konfigurieren, führen Sie in CA IdentityMinder die folgenden Schritte aus:

- Erstellen Sie eine präventive Identitätsrichtlinie mit dem Namen "Manager-Titel für Auftragnehmer" und den folgenden Einstellungen:
  - Richtlinienbedingung: Benutzer wobei (Title = "Manager" and Organization = "Contractor")
  - Aktion zu Richtlinie anwenden: Warnung mit der Meldung "Manager müssen Vollzeitmitarbeiter sein"
- Ändern Sie die Aufgabe "Benutzer ändern" so, dass sie einen Workflow-Prozess mit den folgenden Einstellungen enthält:
  - Workflow-Prozess: Richtlinien-basierend
  - Genehmigungsregelobjekt: Verletzung der Identitätsrichtlinie
  - Identitätsrichtlinie: wobei (Name = "Manager-Titel für Auftragnehmer")
  - Workflow-Prozess: SingleStepApproval

Kombinieren von Identitätsrichtlinien und präventiven Identitätsrichtlinien

Sie können Identitätsrichtlinien und präventive Identitätsrichtlinien kombinieren, um die Anforderungen hinsichtlich der Trennung von Pflichten (Segregation of Duties, SoD) zu erfüllen. In diesem Fall werden Identitätsrichtlinien in Bezug auf bestehende SoD-Verletzungen verwendet, und präventive Identitätsrichtlinien verhindern neue Verletzungen.

Konfigurieren Sie zur Unterstützung dieses Anwendungsfalls einen Identitätsrichtliniensatz mit zwei Typen von Aktionen:

- Aktionen, die während der Benutzersynchronisierung auftreten

  Diese Aktionen führen zu Änderungen an Benutzerattributen, Gruppen- und Rollenmitgliedern, Administratoren oder Eigentümern. Beispielsweise kann eine Aktion dieses Typs einen Benutzer aus einer Rolle entfernen, wenn eine Verletzung erkannt wird.

  Diese Aktionen unterscheiden sich in der Hinsicht von präventiven Aktionen, dass sie nicht beim Senden einer Aufgabe angewendet werden. Sie werden nur während der Benutzersynchronisierung (siehe Seite 488) angewendet.

- Präventive Aktionen

  Diese Aktionen legen fest, wie CA IdentityMinder auf das Auftreten einer Verletzung einer präventiven Identitätsrichtlinie *vor* dem Senden einer Aufgabe reagiert. CA IdentityMinder kann zulassen, dass die Aufgabe gesendet wird, eine Warnung ausgeben und einen Workflow-Prozess auslösen oder das Senden der Aufgabe verhindern.

  In jedem dieser Fälle wird die Verletzung in der Audit-Datenbank aufgezeichnet.

Stellen Sie sich vor, dass ein Unternehmen verhindern möchte, dass Benutzer gleichzeitig die Rollen "Personalleiter" und "Gehaltsgenehmiger" besitzen. Dieses Unternehmen erstellt eine Identitätsrichtlinie mit zwei "Aktion zu Richtlinie anwenden"-Aktionen:

- Entfernen des Benutzers aus der Rolle "Gehaltsgenehmiger"

  Diese Aktion wird ausgeführt, wenn CA IdentityMinder Benutzer mit Identitätsrichtlinien synchronisiert.

  In diesem Fall hat das Unternehmen die Benutzersynchronisierung für die Aufgabe "Benutzer ändern" konfiguriert. Wenn ein Administrator einen Benutzer ändert, wertet CA IdentityMinder alle anwendbaren Identitätsrichtlinien aus und wendet die Aktionen an. In diesem Beispiel entfernt CA IdentityMinder Benutzer, die die Rollen "Personalleiter" und "Gehaltsgenehmiger" besitzen, aus der Rolle "Gehaltsgenehmiger".

- Ablehnen der Aufgabe

  Diese präventive Aktion verhindert, dass Administratoren einer Person diese beiden Rollen zuweisen, indem sie nicht zulässt, dass der Administrator die Aufgabe sendet.

Hinweis: Wenn Sie eine Identitätsrichtlinie mit diesen beiden Aktionstypen konfigurieren, stellen Sie sicher, dass die Aktionen nicht miteinander in Konflikt stehen. Beispielsweise können Sie eine Identitätsrichtlinie konfigurieren, die verhindert, dass Benutzer die Rollen "Manager" und "Auftragnehmer" besitzen. In der Richtlinie geben Sie zwei Aktionen an:

- Eine Warnung, die einen Workflow-Prozess auslöst, der eine Genehmigung erfordert, bevor die Rollen zugewiesen werden, und
- Eine Aktion, die einen Benutzer aus der Rolle "Manager" entfernt

Ein Genehmiger genehmigt die Rollenzuweisung für die Rollen "Manager" und "Auftragnehmer", die zweite Aktion entfernt jedoch den Benutzer aus der Rolle "Manager", wenn die Benutzersynchronisierung ausgeführt wird.

Kapitel 16: Policy Xpress

Dieses Kapitel enthält folgende Themen:

Übersicht über Policy Xpress (siehe Seite 511)
Erstellen einer Richtlinie (siehe Seite 512)

Übersicht über Policy Xpress

Policy Xpress ermöglicht die Erstellung einer komplexen Business Logic (Richtlinien) in CA IdentityMinder, ohne hierfür benutzerdefinierten Code erstellen zu müssen. Allerdings ist die Erstellung von Policy Xpress-Richtlinien komplex und muss daher wohldurchdacht sein und sorgfältig geplant werden. Ein Administrator, der CA IdentityMinder-Portalfenster verwendet, kann eine Richtlinie innerhalb von Policy Xpress konfigurieren, um sogar die speziellste Business Logic zu implementieren. Wenn Geschäftsrichtlinien sich ändern, kann ein Administrator die Richtlinien mithilfe von Konfigurationsfenstern innerhalb von CA IdentityMinder ändern, ohne dass ein Entwickler den zugrundeliegenden Code ändern muss, oder noch wichtiger – mit den geeigneten Änderungsverwaltungsverfahren – ohne Neustart der CA IdentityMinder-Services.

Hinweis: Ausführlichere Informationen zu Policy Xpress finden Sie im Policy Xpress-Wiki https://communities.ca.com/web/ca-identity-and-access-mgmt-distributed-global-user-community/wiki/-/wiki/Main/Policy+Xpress?p_r_p_564233524_categoryId=0&#p_36.

Erstellen einer Richtlinie

Definieren Sie zum Erstellen einer Richtlinie mit Policy Xpress folgende grundlegenden Elemente einer Richtlinie.

Profil

Definiert den Richtlinientyp und die Priorität und ermöglicht das Gruppieren ähnlicher Richtlinien zur einfachen Verwaltung.

Ereignisse

Definieren den Ausführungszeitpunkt einer Richtlinie.

Hinweis: Stellen Sie den Ereignisparameter mit Bedacht ein. Die Business Logic muss zu bestimmten Zeiten ausgeführt werden, um Datenfehler zu verhindern und die Leistung zu erhöhen. Beispielsweise sollte ein Benutzer bei seiner Erstellung auf "Aktiviert" gesetzt werden. Wenn diese Logik zu einem beliebigen Zeitpunkt ausgeführt wird, kann es passieren, dass Benutzerkonten, die deaktiviert sein sollten, wieder aktiviert werden. Ein weiteres Beispiel besteht darin, dem Benutzer eine Bereitstellungsrolle zuzuweisen, die den Zugriff auf ein bestimmtes System ermöglicht. Diese Rolle sollte dem Benutzer nur zugewiesen werden, nachdem eine andere Rolle zugewiesen und genehmigt wurde. Policy Xpress ermöglicht die Aktivierung seiner Business Logic während der Ereignis- und Business Logic Task-Handler-Verarbeitung, ähnlich wie bei benutzerdefinierten Adaptern. Daher kann die Logik, anders als bei Identitätsrichtlinien, jederzeit ausgelöst werden, nicht nur am Anfang einer Aufgabe.

Daten (Datenelemente)

Geben Sie die von der Richtlinie verwendeten Daten an. Jede Art von Business Logic benötigt einige Daten für die Verarbeitung. Diese Daten können verwendet werden, um Entscheidungen zu treffen oder um komplexere Daten zu erstellen.
Policy Xpress bietet viele einzelne Komponenten zum Sammeln von Daten. Diese Komponenten werden als *Datenelemente* bezeichnet. Beispielsweise ist der Attributwert eines Benutzers ein Datenelement. So kann Policy Xpress z. B. den Vornamen des Benutzers erfassen und zur späteren Verwendung als Datenelement speichern.

Eintrittsregeln

Definieren die Anforderungen, die zur Ausführung erfüllt sein müssen. Durch das Definieren von Eintrittsregeln können Sie festlegen, wann Policy Xpress Richtlinien auswertet. Dies kann die Richtlinien vereinfachen und die Leistung verbessern. Eine Eintrittsregel kann z. B. festlegen, dass die Richtlinie "Set Full Name" (Vollständigen Namen festlegen) *nur* ausgeführt wird, wenn sich der Vorname oder der Nachname geändert hat.

Aktionsregeln

Definieren die auf Basis der gesammelten Informationen ergriffene Maßnahme. Beispielsweise kann Policy Xpress auf Basis des Abteilungsnamens eines Benutzers diesem unterschiedliche Rollen zuweisen oder unterschiedliche Kontowerte angeben.

Aktionen

Geben Sie die durchzuführende Aktion an. Am Ende des Prozesses führt Policy Xpress die von der Business Logic benötigten Aktionen durch. In Policy Xpress ist eine Aktionsregel mit mehreren Aktionen verknüpft. Wenn die Regelkriterien erfüllt sind, werden die Aktionen durchgeführt. Aktionen können das Zuweisen von Attributwerten zu einem Benutzer oder einem Konto, das Ausführen einer Befehlszeile, das Ausführen eines SQL-Befehls oder das Generieren eines neuen Ereignisses umfassen.

Profil

Die Registerkarte "Profil" einer Policy Xpress-Richtlinie enthält Felder, die Richtlinien verwalten und die Leistungsmerkmale von Richtlinien verfeinern.

Hinweis: Eine Richtlinie ist nur für die Umgebung gültig, in der sie erstellt wurde. Wenn Sie beispielsweise eine Richtlinie erstellen, während Sie in der neteauto-Umgebung angemeldet sind, wird die Richtlinie nur für die neteauto-Umgebung ausgeführt.

Geben Sie folgende Profilinformationen an, wenn Sie eine Richtlinie erstellen:

Richtlinienname

Definiert einen eindeutigen Anzeigenamen für die Richtlinie.

Richtlinientyp

Definiert die Listener (siehe Seite 515), die die Richtlinie auslösen. Jeder Richtlinientyp hat eine andere Konfiguration.

Hinweis: Sie können dieses Feld nicht mehr ändern, nachdem die Richtlinie gespeichert wurde.

Kategorie

Definiert eine Gruppe verwandter Richtlinien. In diesem Feld können Sie Richtlinien zur einfachen Verwaltung gruppieren.

Beschreibung

Gibt eine Beschreibung der Richtlinie an.

Priorität

Wenn es mehrere Richtlinien gibt, die bei einem einzigen Ereignis ausgeführt werden, gibt dieses Feld an, wann die Richtlinie ausgeführt wird. Richtlinien werden auf der Basis ihrer Priorität ausgeführt. Je niedriger die Nummer ist, desto höher ist die Priorität (Priorität 1 wird zuerst ausgeführt, 10 als zweites, 50 als drittes usw.). Das Festlegen der Priorität ist sinnvoll, wenn Richtlinien voneinander abhängen oder wenn eine komplexe Richtlinie in zwei einfache Richtlinien aufgeteilt wurde, die nacheinander ausgeführt werden.
Angenommen, es werden drei Richtlinien ausgeführt, wenn die Datenbank einen bestimmten Wert enthält. Statt dass jede der Richtlinien den Wert in der Datenbank prüft, können Sie eine Richtlinie erstellen, die vor den drei anderen Richtlinien ausgeführt wird und den Wert prüft. Wenn die neue Richtlinie dem erforderlichen Wert entspricht, kann Policy Xpress eine Variable setzen. Die anderen drei Richtlinien werden nur ausgeführt, wenn diese Variable gesetzt ist, wodurch ein redundanter Zugriff auf die Datenbank verhindert wird.

Aktiviert

Gibt an, ob die Richtlinie in CA IdentityMinder aktiv ist. Sie können die Auswahl dieses Kontrollkästchens aufheben, wenn Sie eine Richtlinie deaktivieren möchten, ohne sie zu löschen.

Einmal ausführen

Gibt an, ob die Richtlinie nur einmal ausgeführt wird. Einige Richtlinien müssen möglicherweise jedes Mal ausgeführt werden, wenn sie Kriterien erfüllen, andere hingegen müssen nur einmal ausgeführt werden. Dieser Wert legt fest, ob Aktionsregeln, die bereits ausgeführt wurden, erneut ausgeführt werden sollen.

Beispielsweise ist das Hinzufügen einer SAP-Rolle zu einem Benutzer auf der Basis der Abteilung eine Aktion, die nur beim ersten Mal, wenn der Benutzer der Abteilung angehört, durchgeführt werden sollte. Hingegen würde eine Richtlinie, die die Gehaltsstufe des Benutzers auf der Basis seines Titels festlegt, *nicht* für die einmalige Ausführung festgelegt werden, um sicherzustellen, dass keine unbefugten Änderungen stattfinden.

Hinweis: Die Option "Einmal ausführen" gilt nur für ein Objekt, nicht global.

Listener

Policy Xpress-Richtlinien werden von Ereignissen im System ausgelöst. Zur Implementierung dieser Funktion benachrichtigen in das System integrierte Listener Policy Xpress, wenn ein Ereignis auftritt, und stellen Details zu diesem Ereignis bereit.

Folgende Listener sind verfügbar:

Ereignis

Hört auf alle Ereignisse im System und alle zugehörigen Status (Vor, Genehmigt, Abgelehnt usw.). Dieser Listener meldet Policy Xpress auch den Namen des Ereignisses. Die folgenden Status sind für den Listener "Ereignis" verfügbar:

- Vor
- Abgelehnt
- Bestätigt
- Nach
- Fehlgeschlagen

UI

Hört auf unterschiedliche im System ausgeführte Aufgaben im synchronisierten Status, d. h. während ein Benutzer sich in der Benutzeroberfläche für die Aufgabe befindet. Die folgenden Status sind für den Listener "UI" verfügbar:

- Start: wenn die Aufgabe startet
- Subjekt festlegen: wenn das primäre Objekt gefunden wird
- Bei Änderung validieren (siehe Seite 516): wenn ein Attribut mit dem Flag "Bei Änderung validieren" geändert wird
- Beim Senden validieren: wenn auf die Schaltfläche "Senden" geklickt wird
- Sendung: wenn die Aufgabe gesendet wird

Workflow

Hört auf Workflow-Prozesse, die Genehmiger gefunden haben. Dieser Listener dient zum Ausführen von Richtlinien, die auf Genehmigern basieren, z. B. zum Senden einer E-Mail an den Genehmiger.

Gesendete Aufgabe

Hört auf gesendete Aufgaben, die nicht im Hintergrund ausgeführt werden. Dieser Listener ähnelt dem Listener "Ereignis", bezieht sich jedoch auf die gesamte Aufgabe, nicht nur auf ihre Ereignisse. Die folgenden Status sind für den Listener "Gesendete Aufgabe" verfügbar:

- Aufgabe gestartet
- Aufgabe abgeschlossen
- Aufgabe fehlgeschlagen

Umgekehrte Synchronisierung

Hört auf Benachrichtigungen im System, die sich auf die Explore-Funktion von CA IdentityMinder beziehen.

Validierung von auf dem Bildschirm angezeigten Attributen

Neben den definierten Auslösern (Richtlinientypen) kann Policy Xpress auch die Validierung von Attributen überwachen. Dadurch können Sie Richtlinien erstellen, die ausgeführt werden, wenn ein als "Bei Änderung validieren" gekennzeichnetes Attribut auf dem Bildschirm aktualisiert wird.

Diese Funktion kann zum Erstellen von abhängigen Dropdown-Listen verwendet werden. Wenn z. B. zwei Dropdown-Listen auf dem Bildschirm angezeigt werden und eine Option der ersten Dropdown-Liste ausgewählt wird, wird Policy Xpress ausgeführt und legt den Wert für die zweite Dropdown-Liste anhand der in der ersten Dropdown-Liste ausgewählten Option fest. Die Anzahl der Dropdown-Listen und anderer Bildschirmaktualisierungen ist nicht begrenzt. Die Dropdown-Liste unterscheidet sich von Auswahlfelddaten, weil sie statt durch Importieren einer XML-Datei mit statischen Optionen durch eine beliebige Logik mit Optionen gefüllt werden kann.

Eine weitere mögliche Verwendung ist das Zuweisen anderer Attribute basierend auf dem Wert eines Attributs. Wenn z. B. ein Administrator eine Abteilung auswählt, kann Policy Xpress andere Attribute automatisch zuweisen, z. B. den Abteilungsleiter, die Abteilungsnummer und den von der Personalabteilung vergebenen Abteilungscode. Dadurch wird das Schreiben von Logical-Attribute-Handler-Code überflüssig.

Konfigurieren der Validierung mit einer Policy Xpress-Richtlinie

1. Ändern Sie das Profilfenster einer Aufgabe in der Benutzerkonsole, und wählen Sie das Feld aus, das Sie überwachen möchten.
2. Greifen Sie auf die Eigenschaften des Feldes zu, und wählen Sie in der Dropdown-Liste "Bei Änderung validieren" die Option "Ja" aus.
3. Erstellen Sie in Policy Xpress eine Richtlinie des Typs UI (siehe Seite 515).
4. Wählen Sie auf der Registerkarte "Bei Ereignis ausführen" den Status "Bei Änderung validieren" und die Aufgabe aus, die Sie in Schritt 1 geändert haben.

Anwendungsfall: nach anstößigen Namen suchen

Wenn ein neuer Benutzer erstellt wird, kann es sinnvoll sein zu überprüfen, ob der Benutzername anstößig ist. Der folgende Vorgang beschreibt, wie mit Hilfe einer Policy Xpress-Richtlinie nach anstößigen Namen gesucht werden kann.

1. Stellen Sie sicher, dass für die entsprechenden Felder im Profilfenster der Aufgabe "Benutzer erstellen" die Option "Bei Änderung validieren" auf "Ja" gesetzt sind.
2. Erstellen Sie in Policy Xpress eine Richtlinie des Typs UI.
3. Wählen Sie auf der Registerkarte "Bei Ereignis ausführen" den Status "Bei Änderung validieren" und die Aufgabe "Benutzer erstellen" aus.
4. Erstellen Sie die folgenden Datenelemente, um den Vornamen zu überprüfen:
   - Vornamenattribut abrufen (Attribute, Benutzerattribut, Abrufen)
   - Vornamen vollständig in Kleinbuchstaben umwandeln (Allgemein, Zeichenfolgenparser, Kleinschreibung)
   - Vornamen anhand anstößiger Worte in einer Datenbanktabelle prüfen (Datenquellen, SQL-Abfragedaten).
5. Erstellen Sie ähnliche Datenelemente wie in Schritt 4, um den Nachnamen zu überprüfen.
6. Erstellen Sie wie folgt eine Aktionsregel:
   - Bedingung: Vorname ist nicht "" (dies tritt auf, wenn die Abfrage eine Meldung zurückgibt, dass der Name anstößig ist)
   - Aktion: angezeigte Meldung (Meldungen, Meldung auf dem Bildschirm) mit dem anstößigen Namen.

   Diese Regel zwingt den Benutzer, den Namen zu ändern, bevor er die Aufgabe "Benutzer erstellen" erneut sendet.
7. Erstellen Sie eine ähnliche Aktionsregel wie in Schritt 6 für den Nachnamen.

Ereignisse

Je nach in der Registerkarte "Profil" ausgewähltem Richtlinientyp können Sie Aktivierungszeiten konfigurieren, um festzulegen, wann die Richtlinie ausgewertet wird. Z. B. kann eine Richtlinie vom Typ "Ereignis" für die Auswertung vor einem "CreateUserEvent" festgelegt werden. Eine Richtlinie vom Typ "Aufgabe" kann für die Auswertung zum Zeitpunkt der Subjektfestlegung für "DisableUserEvent" festgelegt werden.

Wählen Sie zum Konfigurieren einer Aktivierungszeit folgende Felder aus:

Zustand

Gibt den Zeitrahmen oder die Aktion an, die mit dem Ereignis zusammenhängt, das die Richtlinie aktiviert. Beispielsweise kann festgelegt werden, dass eine Richtlinie "Vor" dem Eintreten eines Ereignisses ausgeführt wird.

Ereignisname

Gibt das Ereignis an, das die Richtlinie aktiviert, z. B. "CreateUserEvent".

Eine Richtlinie kann mehrere Aktivierungszeiten haben. Immer wenn eine angegebene Aktivierungszeit (ein Status und ein Ereignis) im System auftritt, sucht Policy Xpress alle Richtlinien mit dieser Aktivierungszeit und wertet sie auf der Basis ihrer Reihenfolge aus.

Hinweis: Wenn eine Richtlinie mit einer Aktivierungszeit übereinstimmt, die im System auftritt, bedeutet dies nicht, dass sie automatisch ausgeführt wird. Später im Prozess ausgewählte Regelkriterien legen fest, ob die Richtlinie abgeschlossen ist.

Datenelemente

Datenelemente werden zum Erstellen von Richtliniendaten verwendet. Eine Richtlinie kann mehrere Datenelemente enthalten, die die von der Richtlinie verwendeten Informationen darstellen.

Policy Xpress verwendet flexible Plugins zum Sammeln der Datenelementinformationen. Jedes Plugin kann eine kleine dedizierte Aufgabe durchführen. Jedoch können mehrere Plugins zusammen verwendet werden, um komplexere Richtlinien zu erstellen. Beispielsweise ist ein Benutzerattributelement ein Datenelement-Plugin. Ziel des Elements ist es, Informationen über ein bestimmtes Attribut zu sammeln, das Teil des Benutzerprofils ist.

Datenelemente werden berechnet, wenn sie aufgerufen werden, also entweder, wenn eine Regel das Datenelement verwendet oder wenn ein anderes zu berechnendes Element das Datenelement als Parameter verwendet.
Ein SQL-Abfragedatenelement kann beispielsweise einen Wert aus einer Tabelle abrufen, benötigt aber die Abteilung des Benutzers, um die Abfrage zu erstellen. In diesem Fall muss das Abteilungs-Datenelement vor dem SQL-Abfragedatenelement ausgeführt werden, so dass anschließend der Wert als Parameter verwendet werden kann (siehe Seite 521).

Folgende Felder definieren ein Datenelement:

Name

Definiert einen angezeigten Namen, der das Datenelement beschreibt. Einige Datenelemente sind komplex (z. B. das Abrufen von Variablen oder von Informationen aus der Datenbank). Wählen Sie daher einen aussagekräftigen Namen, um die Verwaltung der Datenelement zu vereinfachen.

Kategorie

Ermöglicht die Gruppierung von Datenelementen. Dieses Feld sortiert die Datenelemente und vereinfacht die Auswahl.

Typ

Gibt den Datenelementtyp mit dem jeweiligen dedizierten Verwendungszweck an. Dieses Feld basiert auf der ausgewählten Kategorie.

Funktion

Definiert mögliche Variationen derselben Daten. Die meisten Datenelemente unterstützen nur die Get-Funktion.

Angenommen, das Benutzerattribut-Datenelement hat folgende Funktionen:

- Get (Abrufen): gibt die Werte des Attributs zurück
- ist mehrwertig: gibt "true" (wahr) zurück, wenn der Wert mehrwertig ist
- ist logisch: gibt "true" (wahr) zurück, wenn der Wert logisch ist

Funktionsbeschreibung

Bietet eine vordefinierte Beschreibung der Funktion. Jede ausgewählte Funktion bietet eine andere Beschreibung, um ihren Verwendungszweck und die erwarteten Werte zu erläutern.

Parameter

Definiert die an das Datenelement übergebenen Parameter. Datenelement sind dynamisch und können je nach Parameter unterschiedliche Dinge tun. Ein Benutzerattribut-Datenelement liefert je nach ausgewähltem Attribut unterschiedliche Ergebnisse. Die Untertypoption definert zudem die Anzahl der Parameter, ihre Namen und die optionalen Werte, sofern verfügbar.

Sie können bei Bedarf zusätzliche Parameter hinzufügen. Das SQL-Abfragebeispiel akzeptiert zwei erforderliche Parameter: die Datenquelle und die Abfrage selbst. Die Abfrage kann das "?" als Platzhalter für Werte verwenden (wie bei einer Prepared-Anweisung). Durch Hinzufügen weiterer Parameter können Sie diese Werte festlegen.

Hinweis: Wenn Sie Datenelemente in Policy Xpress anzeigen, sehen Sie eine Spalte mit dem Titel "Im Einsatz". Ein Häkchen in dieser Spalte bedeutet, dass das Datenelement von einer Regel, einem Aktionsparameter oder als Parameter für andere Datenelemente verwendet wird.

Verwenden dynamischer Werte in Daten- oder Aktionselementen

Dynamische Werte sind das Ergebnis berechneter Datenelemente. Ihre Werte werden erst zur Laufzeit festgelegt. Diese Werte können dann als Parameter anderer Datenelemente (deren Berechnung nachträglich auf Basis der Priorität erfolgt) verwendet werden.

So verwenden Sie einen dynamischen Wert als Parameter eines Datenelements

1. Suchen Sie in der Registerkarte "Richtliniendaten" den Parameter, für den Sie einen dynamischen Wert festlegen möchten.
2. Geben Sie im leeren Textfeld einen beliebigen, normalen Text ein, oder wählen Sie den dynamischen Wert aus der rechten Dropdown-Liste aus.
3. Klicken Sie auf "OK".

Variablen

Policy Xpress verfügt über Variablen, die mit Aktionen festgelegt werden und als Datenelemente gespeichert werden (Variablenkategorie). Variablen werden von allen gleichzeitig ausgeführten Richtlinien gemeinsam genutzt. Daher kann eine festgelegte Variable von anderen Richtlinien verwenden werden, die eine niedrigere Priorität haben.

Eine Variable kann z. B. einen Wert enthalten, der von einer Richtlinie einmal berechnet wurde und dann von anderen Richtlinien gemeinsam genutzt wird, die dadurch den Wert nicht erneut berechnen müssen. Die erste Richtlinie weist der Variable einen Wert zu. Die später ausgeführten Richtlinien lesen diesen Wert mit Hilfe eines Datenelements ein, das den Variablennamen als Parameter besitzt.

Eine Variable kann auch ein Auslöser für andere Richtlinien sein. In diesem Fall werden die Richtlinien nur ausgeführt, wenn die erste Richtlinie ausgeführt wurde.

Eintrittsregeln

Eintrittsregeln definieren die Bedingungen für den Zeitpunkt der Ausführung einer Richtlinie. Diese Bedingungen verwenden die Werte, die von den Datenelementen in der Richtlinie gesammelt wurden.

Es kann mehrere Eintrittsregeln in einer Richtlinie geben, und eine Eintrittsregel kann mehrere Bedingungen haben. Mindestens eine Eintrittsregel muss übereinstimmen, d. h. *alle* Bedingungen in dieser Eintrittsregel müssen erfüllt sein, damit eine Richtlinie mit den Aktionsregeln fortfährt.

Eine Eintrittsregel wird durch folgende Felder definiert:

Name

Gibt einen Anzeigenamen für die Eintrittsregel an.

Beschreibung

Definiert die Bedeutung der Eintrittsregel.

Bedingungen

Gibt die zu erfüllenden Kriterien an.

Hinweis: Bedingungen in einer Eintrittsregel sind immer durch einen UND-Operator verbunden.

Weitere Informationen:

Bedingungen (siehe Seite 522)

Bedingungen

Eine Bedingung wird in Eintritts- und Aktionsregeln verwendet und besteht aus den folgenden Komponenten:

- Richtliniendaten
- Operator
- Wert

Sie möchten beispielsweise eine Bedingung erstellen, die überprüft, ob die Abteilung eines Benutzers geändert wurde. Definieren Sie zuerst ein Datenelement "Abteilung geändert", wählen Sie es dann als Bedingung aus, legen Sie "Equals" (Gleich) als Operator fest und setzen Sie den Wert auf "True" (Wahr).

Weitere Informationen:

Eintrittsregeln (siehe Seite 521)
Aktionsregeln (siehe Seite 522)

Aktionsregeln

Aktionsregeln haben eine ähnliche Struktur wie Eintrittsregeln, funktionieren jedoch anders. Aktionsregeln legen fest, wann eine Aktion durchgeführt werden soll. Wenn beispielsweise eine Richtlinie eine Aktion ausführen soll, wenn sich die Abteilung eines Benutzers in "Vertrieb" geändert hat, erstellen Sie eine Aktionsregel, die "Department = Sales" definiert.

Außerdem ist es möglich, dass statt aller Bedingungen einer Eintrittsregel die Kriterien mehrerer Aktionsregeln erfüllt werden. Die Aktionsregel mit der höchste Priorität (0 ist am höchsten) ist die *einzige*, die verwendet wird.

Aktionsregeln können auch eine oder mehrere Aktionen enthalten, und die Aktionen sind in Hinzufügeaktionen und Entfernaktionen aufgeteilt.

Eine Aktionsregel wird durch folgende Felder definiert:

Name

Gibt einen Anzeigenamen für die Aktionsregel an. Dieser Name muss eindeutig sein.

Beschreibung

Definiert die Bedeutung der Aktionsregel.

Bedingungen

Gibt die zu erfüllenden Kriterien an.

Priorität

Definiert, welche Aktionsregel ausgeführt wird, falls mehrere Aktionsregeln übereinstimmen. Dieses Feld ist zum Definieren von Standardaktionen hilfreich. Wenn Sie beispielsweise mehrere Regeln haben, jeweils eine für einen Abteilungsnamen, ist es möglich, eine Standardaktion festzulegen, indem Sie eine zusätzliche Regel ohne Bedingungen, aber mit einer niedrigeren Priorität (z. B. 10, wenn alle anderen 5 haben) hinzufügen. Wenn für keine der Abteilungsregeln eine Übereinstimmung gefunden wird, wird die Standardaktion verwendet.

Aktionen hinzufügen

Definiert eine Liste der Aktionen, die bei Übereinstimmung der Regel durchgeführt werden. Sie können z. B. eine Regel konfigurieren, nach der bei Übereinstimmung der Abteilung des Benutzers mit der in der Bedingung konfigurierten Abteilung eine spezifische Active Directory-Gruppe hinzugefügt wird. Aktionsregeln verhalten sich unterschiedlich, je nach der Einstellung "Einmal ausführen". Wenn die Richtlinie auf "Einmal ausführen" gesetzt ist, werden die zugehörigen Aktionen bei der ersten Übereinstimmung der Regel ausgeführt. Die Aktionen werden nicht erneut für jede weitere Regelübereinstimmung ausgeführt. Im obigen Beispiel wird die Active Directory-Gruppe nur einmal zum Benutzer hinzugefügt. Wenn "Einmal ausführen" nicht festgelegt ist, werden die Aktionen so oft ausgeführt, wie es Übereinstimmungen mit der Regel gibt. Dieses Feld ist für das Erzwingen von Werten wichtig.

Entfernaktionen

Definiert eine Liste der Aktionen, die ausgeführt werden sollen, wenn die Bedingungen der Regel nicht mehr erfüllt werden. Beispielsweise wurde im vorigen Beispiel eine Active Directory-Gruppe abhängig von der Abteilung zum Benutzer hinzugefügt. Wenn die Abteilung geändert wird, entfernt die Aktion für das Entfernen die Active Directory-Gruppe.

Weitere Informationen:

Bedingungen (siehe Seite 522)

Aktionen

Aktionen führen die Business Logic aus, wenn die Entscheidungsfindung abgeschlossen wurde. Eine Aktion funktioniert abgesehen vom Ende ähnlich wie Datenelemente. Wenn sie ausgeführt wird, wird kein Wert wiedergegeben, sondern eine Aufgabe durchgeführt.

Hinweis: Aktionen werden in der Reihenfolge ausgeführt, in der sie in der Benutzerkonsole aufgeführt sind.

Eine Aktion wird durch folgende Felder definiert:

Aktionsname

Gibt den Zweck der Aktion an.

Kategorie

Ermöglicht die Gruppierung von Aktionen. Dieses Feld sortiert die Aktionen und vereinfacht die Auswahl.

Typ und Funktion

Gibt den Typ und die Funktion der ausgeführten Aktion an.

Hinweis: Weitere Informationen zu Typ und Funktion finden Sie unter "Daten".

Funktionsbeschreibung

Bietet eine vordefinierte Beschreibung der Funktion. Jede ausgewählte Funktion bietet eine andere Beschreibung, um ihren Verwendungszweck und die erwarteten Werte zu erläutern.

Parameter

Definiert die an die Aktion übergebenen Parameter.

Flusskontrolle

Standardmäßig werden Richtlinien nach Priorität sortiert und anschließend nacheinander ausgewertet. Dieser Fluss ist zwar fast immer sinnvoll, Sie können den Fluss jedoch bei Bedarf ändern.

Die Funktion zum Ändern des Flusses wird von einer Aktion dargestellt, die an jede Aktionsregel angehängt werden kann. Sie finden Funktionen zum Ändern des Flusses in der Kategorie "System" der Aktion.

Wichtig! Vorsicht beim Ändern von Prozessabläufen. Die Verwendung dieser Aktionen kann zu einer Endlosschleife führen. Wenn Sie beispielsweise "Aktuelle Richtlinie erneut ausführen" für eine Aktionsregel ohne Bedingungen festlegen, ist die Regel immer wahr, und die Richtlinie startet immer wieder neu, ohne beendet zu werden.

Die folgenden vier Funktionen zur Flussänderung können verwendet werden:

Verarbeitung stoppen

Legt fest, dass alle Richtlinien nach der aktuellen Richtlinie ignoriert werden, und beendet Policy Xpress.
Hinweis: Nur Policy Xpress wird beendet. Wenn Sie CA IdentityMinder zwingen möchten, ebenfalls anzuhalten, können Sie das Aktions-Plugin "Ausnahmetyp" verwenden.

Alle Richtlinien neu starten

Hält die Verarbeitung der übrigen Richtlinien an und kehrt zum Anfang der Liste zurück. Diese Option ist nützlich, wenn die Aktion einer Richtlinie die Eingangskriterien einer davor aufgelisteten Richtlinie erfüllt, die noch nicht ausgeführt wurde. Diese Richtlinie wird jetzt neu ausgewertet.

Aktuelle Richtlinie erneut ausführen

Veranlasst die erneute Ausführung einer Richtlinie. Diese Option kann für die Iteration verwendet werden. Beispielsweise muss eine Richtlinie zum Erstellen eines eindeutigen Benutzernamens wiederholt ausgeführt werden, bis sie einen eindeutigen Namen findet.

Zu bestimmter Richtlinie wechseln

Diese Aktion setzt die Auswahl einer vorhandenen Richtlinie voraus. Wenn diese Richtlinie gleichzeitig mit der aktuellen Richtlinie ausgeführt wird (oder davor bzw. danach), wechselt Policy Xpress zur ausgewählten Richtlinie. Wenn die neue Richtlinie eine niedrigere Priorität hat, werden alle Richtlinien zwischen der aktuellen Richtlinie und der ausgewählten Richtlinie ignoriert. Wenn die Priorität der neuen Richtlinie höher ist, wechselt der Prozess zurück.

Hinweis: Vorsicht bei der Verwendung dieses Aktionstyps, da Policy Xpress dadurch möglicherweise bestimmte Richtlinien überspringt.

Festlegen von Fähigkeitsattributen

Wenn Sie eine Aktion "Hinzufügen" erstellen, um ein Funktionsattribut in Policy Xpress festzulegen, wird ein spezifisches Format verwendet, um das Funktionsattribut darzustellen. Die folgenden zwei Formattypen können Funktionsattribute in CA IdentityMinder darstellen:

- Zum Darstellen einfacher Beziehungen, z. B. Active Directory-Gruppen:
  `NativeGroup=Administrators,Container=Builtin,EndPoint=LocalAD,Namespace=ActiveDirectory,Domain=im,Server=Server`
- Zum Darstellen bindender Beziehungen, z. B. SAP-Rollen:
  `{"validFromDate":"2009\/12\/01","roleName":"SAPRole=SAP_AUDITOR_ADMIN,EndPoint=sap endpoint,Namespace=SAP R3,Domain=im,Server=Server","validToDate":"2009\/12\/31"}`

Erstellen Sie ein Datenelement, das den Wert des Funktionsattributs abruft, um das Format eines Funktionsattributs herauszufinden. Der zurückgegebene Wert hat das Format, das Sie in der Aktion "Hinzufügen" verwenden, um das Funktionsattribut festzulegen.

Beispiel: Das Active Directory-Gruppen-Attribut

1. Erstellen Sie eine Policy Xpress-Richtlinie mit den folgenden Einstellungen:
   - Richtlinientyp: Ereignis
   - Ereignisse: Nach – Benutzer ändern
2. Konfigurieren Sie die folgende Aktion "Hinzufügen" in der Aktionsregel:
   - Kategorie: Attribute
   - Typ: Kontodaten festlegen
   - Funktion: Festlegen
   - Endpunkttyp: Active Directory
   - Endpunkt: *Endpunktname*
   - Kontoname: *Konto*
   - Attribut: Mitglied von (groupMembership)
   - Wert:
     NativeGroup=Administrators,Container=Builtin,Endpoint=*Endpunkt_Name*,Namespace=ActiveDirectory,Domain=im,Server=Server

Erweitert

Policy Xpress ermöglicht viele unterschiedliche Konfigurationen und interagiert auch mit externen Komponenten. Aufgrund dieser Flexibilität können Fehler auftreten, die nicht unbedingt Programmfehler sind, z. B. eine nicht richtig konfigurierte Datenquelle, ein fehlender Wert von einem dynamischen Datenelement oder ein Endpunkt, der nicht antwortet.

In der Regel hält das System die Berechnung der Richtlinien für den aktuellen Schritt an, wenn ein Fehler auftritt. Sie können die vorgegebene Reaktion auf Fehler jedoch basierend auf der Fehlerkategorie ändern. Wenn Sie beispielsweise eine Richtlinie haben, die nicht kritisch ist, können Sie definieren, dass der Vorgang bei einem Fehler fortgeführt wird.

Sie können die vorgegebene Reaktion auf Fehler bei Bedarf auf der Registerkarte "Erweitert" anpassen.

Hinweis: Es wird empfohlen, diese Reaktionen auf Fehler auf den Standardwerten zu belassen. Für erweiterte Anwendungsfälle können diese Einstellungen jedoch für einzelne Richtlinien geändert werden. Wenn Sie beispielsweise eine Richtlinie haben, die nicht kritisch ist, können Sie definieren, dass der Vorgang trotz eines Fehlers der Richtlinie fortgeführt wird.

Die folgenden Fehlerkategorien können auf der Registerkarte konfiguriert werden:

- Validierung: tritt auf, wenn falsche Informationen an ein Plugin gesendet wurden. Dieser Fehlertyp wird gemeldet, bevor die Ausführung der Aktion versucht wird.
- Umgebung: wird von Problemen in der Umgebung verursacht, z. B. einem Fehler im Datenbankserver für das SQL-Plugin
- Zugelassen: ein nicht kritischer Fehler. Bei diesem Fehlertyp wird die Anfrage standardmäßig weiter verarbeitet, z. B. wenn das Senden einer E-Mail fehlschlägt.

Für alle genannten Fehler können die folgenden Optionen festgelegt werden:

- Ereignis fehlgeschlagen: hält die aktuelle Aktion an. Dies ist die Standardeinstellung für die meisten Fehlertypen.
- Richtlinie fehlgeschlagen: hält die aktuelle Richtlinie und alle zugehörigen Aktionen an. Die anderen Richtlinien werden verarbeitet.
- Ignorieren: protokolliert alle Fehler, aber hält die Aktionen oder Richtlinien nicht an

Kapitel 17: Mobile CA IdentityMinder-App

Die mobile CA IdentityMinder-App befähigt Sie, Ihre bestehende CA IdentityMinder-Infrastruktur so einzusetzen, dass Benutzer die folgenden Aufgaben über ein mobiles Gerät wie einem Smartphone oder Tablet ausführen können:

- Zurücksetzen von vergessenen Kennwörtern
- Ändern eines Kennworts
- Reagieren auf Genehmigungsanforderungen
- Anzeigen von Benutzerinformationen

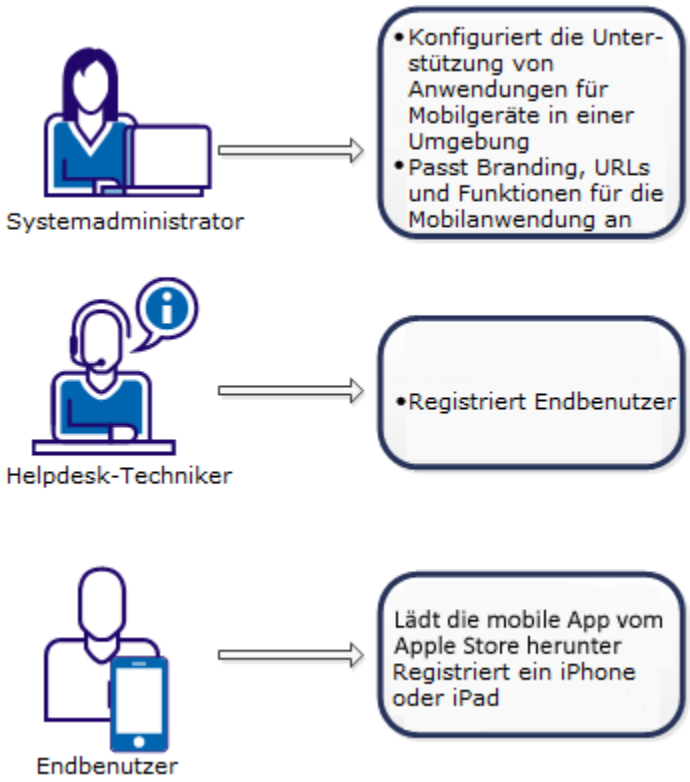
  Mit dieser Funktion können Benutzer Informationen zu anderen Benutzern in der Organisation anzeigen. Zum Beispiel können Genehmiger von Arbeitselementen grundlegende Informationen zum Manager eines Benutzers, wie Name und Adresse, anzeigen, bevor sie über die Genehmigung entscheiden. Wenn weitere Informationen erforderlich sind, kann der Genehmiger auf einen Link klicken, um das vollständige Profil anzuzeigen.

Dieses Kapitel enthält folgende Themen:

Funktionsweise der Implementierung (siehe Seite 530)
So konfigurieren Sie CA IdentityMinder zur Unterstützung mobiler Apps (siehe Seite 531)
Konfigurieren einer mobilen App (siehe Seite 537)
Download der mobilen App (siehe Seite 539)
Fehlerbehebung bei mobilen Apps (siehe Seite 540)

Funktionsweise der Implementierung

Beim Konfigurieren mobiler Apps werden drei Arten von Benutzern eingerichtet. Die folgende Grafik veranschaulicht diese Benutzerarten und die Aufgaben, die sie ausführen.


Systemadministrator
•Konfiguriert die Unterstützung von Anwendungen für Mobilgeräte in einer Umgebung
•Passt Branding, URLs und Funktionen für die Mobilanwendung an
Helpdesk-Techniker
•Registriert Endbenutzer
Endbenutzer
Lädt die mobile App vom Apple Store herunter
Registriert ein iPhone oder iPad

Damit ein Endbenutzer die mobile App mit CA IdentityMinder verwenden kann, werden die folgenden Aktivitäten durchgeführt:

1. Ein Systemadministrator konfiguriert die Unterstützung für die mobile App in einer Umgebung.

   Die Konfiguration umfasst die folgenden Aktivitäten:

   - Konfiguriert Aktivierungs- und Zurücksetzungscode-Attribute
   - Fügt Aufgaben, Policy Xpress-Richtlinien und eine E-Mail-Vorlage für die Registrierung mobiler Benutzer hinzu
   - Erstellt eine Webservice-Definition
   - Ändert die Registrierungs-E-Mail

   Der Systemadministrator konfiguriert auch das Branding, URLs und Funktionen, auf die bzw. das mobile Benutzer zugreifen können.

2. Ein Administrator, zum Beispiel ein Helpdesk-Techniker, registriert die entsprechenden Endbenutzer in der Benutzerkonsole.

   Der Registrierungsprozess löst einen Aktivierungscode für jeden Endbenutzer aus und sendet automatisch eine E-Mail mit den Code- und Registrierungsanweisungen an den Endbenutzer.

3. Der Endbenutzer lädt die mobile App vom Apple Store herunter und registriert ein Gerät, zum Beispiel ein Smartphone oder einen Tablet, anhand der Anweisungen und des Codes, die bzw. den er per E-Mail erhalten hat.

   Der Endbenutzer kann die mobile App dann verwenden, um auf die CA IdentityMinder-Funktionen zuzugreifen.

   Hinweis: Wenn die Option "Kennwort muss geändert werden" während der Benutzererstellung aktiviert wird, können die Benutzer einer mobilen App die Aktivierung nicht abschließen.

So konfigurieren Sie CA IdentityMinder zur Unterstützung mobiler Apps

Die mobile App kommuniziert mit CA IdentityMinder (unter Verwendung von REST-Webservices), um Kennwörter und Genehmigungen zu verwalten. Zur Aktivierung dieser Kommunikation führt ein Systemadministrator die folgenden Schritte durch:

1. Konfigurieren Sie erforderliche Attribute (siehe Seite 532).
2. Fügen Sie einer Umgebung neue Aufgaben hinzu, indem Sie Rollendefinitionsdateien importieren (siehe Seite 534).
3. Erstellen Sie einen Webservice (siehe Seite 535).
4. Ändern Sie die Registrierungs-E-Mail (siehe Seite 536).

Konfigurieren von erforderlichen Attributen

Der CA IdentityMinder-Benutzerspeicher muss die folgenden bekannten Attribute enthalten, um die Benutzerregistrierung und den Zugriff über die mobile App zu ermöglichen:

- %ACTCODE% — Identifiziert das Attribut, das eine nach dem Zufallsprinzip generierte Aktivierungsnummer speichert. Nachdem der Benutzer registriert wurde, enthält dieses Attribut den Begriff "Registriert".
- %ACTCODEVAL% — Identifiziert das Attribut, das den Aktivierungscode speichert, den der Client zum Zeitpunkt der Registrierung festlegt. CA IdentityMinder vergleicht diesen Wert mit dem Wert von %ACTCODE%.
- %PWRESETCODE% — Identifiziert das Attribut, das einen verschlüsselten Code speichert, der Einzelfaktor-Authentifizierung während der Zurücksetzung eines Kennworts bereitstellt.

Ordnen Sie diese bekannten Attribute verfügbaren Benutzerspeicherattributen in der Verzeichniskonfigurationsdatei (directory.xml) zu. Wenn es keine verfügbaren Attribute gibt, erweitern Sie das Benutzerspeicherschema. Weitere Informationen zum Erweitern des Schemas finden Sie in der Dokumentation für Ihren Benutzerspeicher.

Schließen Sie die folgenden Datenklassifizierungen in den Attributbeschreibungen ein:

<DataClassification name="sensitive"/>

Ersetzt den Zurücksetzungscode-Wert durch Platzhalterzeichen in Aufgabenfenstern, Auditdatensätzen und Systemprotokollen.

Wichtig! Schließen Sie die Klassifizierung von vertraulichen Daten nicht in der %ACTCODE%-Attributdefinition ein. Wenn Sie das Attribut für vertrauliche Daten einschließen, funktioniert die mobile App nicht richtig.

<DataClassification name=" AttributeLevelEncrypt "/>

Verschlüsselt und entschlüsselt den Zurücksetzungscode-Wert, während er in den bzw. aus dem Benutzerspeicher mithilfe des definierten Verschlüsselungscodes geschrieben und gelesen wird.

<DataClassification name=" ignore_on_copy "/>

Hat zur Folge, dass CA IdentityMinder ein Attribut ignoriert, wenn ein Administrator eine Kopie eines Objekts in der Benutzerkonsole erstellt.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Management-Konsole an.
2. Wählen Sie "Verzeichnisse" aus, und klicken Sie dann auf das Verzeichnis, das mobile Benutzer enthält.
3. Exportieren Sie das Verzeichnis.
4. Fügen Sie eine Attributbeschreibung hinzu, oder ändern Sie diese, um das bekannte Attribut %ACTCODE% einzuschließen.

Sie können jedes verfügbares Attribut dem bekannten Attribut %ACTCODE% zuordnen.

```
<ImsManagedObjectAttr
physicalname="attr1"
displayname="ActivationCode"
description="Activiation Code"
valuetype="String"
required="false"
multivalued="false"
wellknown="%ACTCODE%"
maxlength="0"
hidden="true"
system="true">
   <DataClassification name="ignore_on_copy"/>
   <DataClassification name=" AttributeLevelEncrypt"/>
   </ImsManagedObjectAttr>
```

5. Wiederholen Sie Schritt 4, um das bekannte Attribut %ACTCODEVAL% zu definieren. Schließen Sie die folgenden Datenklassifizierungen ein:

```
<DataClassification name="sensitive"/>
<DataClassification name="ignore_on_copy"/>
<DataClassification name=" AttributeLevelEncrypt"/>
```

6. Fügen Sie eine Attributbeschreibung für das bekannte Attribut %PWRESETCODE% hinzu. Schließen Sie die folgenden Datenklassifizierungen ein:

```
<DataClassification name="sensitive"/>
<DataClassification name="ignore_on_copy"/>
<DataClassification name=" AttributeLevelEncrypt"/>
```

   Die Attributdefinition ähnelt dem folgenden Beispiel:

```
<ImsManagedObjectAttr
physicalname="XXXX"
description="Password Reset Code"
displayname="Password Reset Code"
valuetype="String"
wellknown="%PWRESETCODE%"
maxlength="0"
hidden="true"
system="true">
   <DataClassification name="ignore_on_copy"/>
   <DataClassification name="sensitive"/>
   <DataClassification name=" AttributeLevelEncrypt"/>
</ImsManagedObjectAttr>
```

7. Speichern Sie die Datei "directory.xml".
8. Laden Sie die gespeicherte Datei "directory.xml", indem Sie in der Management-Konsole auf der Seite "Directory Properties" (Verzeichniseigenschaften) auf "Update" (Aktualisieren) klicken.

Importieren von Admin-Aufgaben

Administratoren registrieren mobile Benutzer in der Benutzerkonsole, damit sich diese bei CA IdentityMinder anmelden können. Der Registrierungsprozess generiert einen Aktivierungscode und sendet eine E-Mail an den mobilen Benutzer.

Um diese Aktivitäten zu unterstützen, importieren Sie eine Rollendefinitionsdatei, die die folgenden Funktionen in einer Umgebung hinzufügt:

- Mobile Konfigurationsaufgaben
- Registrieren von Benutzern für mobile Apps und Entfernen von Benutzern aus mobilen App-Aufgaben
- Policy Xpress-Richtlinien, die Aktivierungscodes generieren und die Registrierung des mobilen Clients in einem Benutzerkonto aufheben
- Eine E-Mail-Vorlage, um die E-Mail an mobile Benutzer zu senden

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Management-Konsole an.
2. Wählen Sie "Environments" (Umgebungen) aus, und klicken Sie dann auf die Umgebung, die die mobile App unterstützt.
3. Wählen Sie "Role and Task Settings" (Rollen- und Aufgabeneinstellungen) aus, und klicken Sie im nächsten Fenster auf "Importieren".
4. Wählen Sie "MobileApp-RoleDefinitions" aus, und klicken Sie dann auf "Fertig stellen".
5. Starten Sie die Umgebung neu.
6. Fügen Sie die folgenden Aufgaben der Rolle des Systemmanagers hinzu:
   - Erstellen einer mobilen Konfiguration
   - Ändern einer mobilen Konfiguration
   - Anzeigen einer mobilen Konfiguration
   - Löschen einer mobilen Konfiguration
   - Registrieren von Benutzern für mobile Apps
   - Entfernen von Benutzern aus mobilen Apps

   Die neuen Aufgaben befinden sich in den Kategorien "Benutzer" und "System".

Erstellen einer Webservices-Konfiguration

Die mobile App verwendet REST-Webservices für die Kommunikation mit CA IdentityMinder. Um die mobile App zu unterstützen, erstellt ein Systemadministrator eine Webservice-Definition in der Benutzerkonsole.

Hinweis: REST-Aufrufe funktionieren nicht, wenn die Verschlüsselung in der Webservice-Konfiguration aktiviert ist.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole als Benutzer mit Systemadministrator-Rechten an.
2. Erstellen Sie eine Webservice-Definition wie folgt:
   a. Öffnen Sie "System", "WebServices", "Webservices-Konfiguration erstellen".
   b. Füllen Sie die folgenden Felder auf der Registerkarte "Profil" aus:
      - Name: *beliebiger Name.* Beispiel: RestMobile
      - Kennung: *eindeutige Kennung.* Der Standardwert ist RestMobile.

        Der Wert des Felds "Kennung" muss mit dem **restid**-Wert in der Konfiguration der mobilen App übereinstimmen.

        Ziehen Sie in Erwägung, den Wert der Kennung und den restid-Wert zu ändern, um die Sicherheit zu erhöhen.
      - Enable Attribute (Attribut aktivieren): Aktivieren Sie dieses Kontrollkästchen.

   c. Füllen Sie die folgenden Felder auf der Registerkarte "Sicherheit" aus:
      - Wählen Sie "Sichere Kommunikation erforderlich" aus.
      - Vergewissern Sie sich, dass "Verschlüsselung aktivieren" nicht aktiviert ist.

        Wenn die Verschlüsselung aktiviert ist, werden keine Benutzerdetails in der mobilen App angezeigt.

   d. Navigieren Sie auf der Registerkarte "Objekttypen" zu BENUTZER, wählen Sie BENUTZER aus, und klicken Sie auf die Schaltfläche "Bearbeiten".
   e. Wählen Sie nur "Ansichtszugriff erlauben" aus.

      Entfernen Sie andere Zugriffsberechtigungen, indem Sie die Optionen "Änderungszugriff erlauben", "Erstellungszugriff erlauben" und "Löschzugriff erlauben" löschen.

f. Führen Sie auf der Registerkarte "Selbstverwaltung" die folgenden Schritte aus:

- Wählen Sie die Schaltfläche "Hinzufügen" unter "Mitgliederregel" aus, um eine Mitgliederrolle zu erstellen und geben Sie "alle" an.

  Hinweis: Sie können nur eine Mitgliederregel erstellen.

- Aktivieren Sie zur Unterstützung der Funktion "Kennwort ändern" in der mobilen App das Zurücksetzen des Kennworts.

g. Richten Sie auf der Registerkarte "Mitglied" eine Mitgliederregel mit den folgenden Kriterien ein:

- Aktivierungscode = Registriert oder
- Aktivierungscode > 0

h. Senden Sie den Webservice, und speichern Sie ihn.

Ändern der Registrierungs-E-Mail

Bearbeiten Sie die standardmäßige Registrierungs-E-Mail, um die URL für das mobile Konfigurationsobjekt einzuschließen.

Gehen Sie wie folgt vor:

1. Wählen Sie in der Benutzerkonsole "System", "E-Mail" und "Modify Email" (E-Mail ändern) aus.
2. Suchen Sie nach dem registrierten Benutzer für die mobile App-E-Mail, und wählen Sie ihn aus.
3. Klicken Sie auf der Registerkarte "Inhalt" auf die Schaltfläche "Toggle HTML Source" (HTML-Quelle ein-/ausschalten).
4. Geben Sie die URL für das mobile Konfigurationsobjekt im href-Eintrag für "mobileregservidm" folgendermaßen an:

   <a href="mobileregservidm://{'Attribute:%ACTCODE%'}&https://FQN/iam/im/ws/Alias/mobile/ConfigName">

   FQN

   Geben Sie den Namen oder die IP-Adresse des CA IdentityMinder-Servers an.

   Alias

   Geben Sie den Namen der Umgebung an.

   ConfigName

   Geben Sie den Namen des Konfigurationsobjekts an.
5. Klicken Sie auf "Senden".

Konfigurieren einer mobilen App

Systemadministratoren konfigurieren die mobile CA IdentityMinder-App in der Benutzerkonsole.

Eine Umgebung kann mehrere Konfigurationen der mobilen App enthalten. Das Erstellen verschiedener Konfigurationen ermöglicht es Ihnen, verschiedenes Branding oder verschiedene Funktionen für verschiedene Typen von mobilen Benutzern zu unterstützen. Zum Beispiel können Sie eine Konfiguration für Kennwortänderungen von Mitarbeitern erstellen, und Sie können eine andere Konfiguration erstellen, mit der Manager Arbeitselemente genehmigen können.

Administratoren können folgende Eigenschaften für die mobile App konfigurieren:

- Branding

  Geben Sie das Unternehmenslogo in der mobilen App an.

- Funktionen

  Aktivieren Sie die folgenden Funktionen:

  - Support bei vergessenen Kennwörtern
  - Support beim Zurücksetzen von Kennwörtern
  - Warteschlange für Workflow-Genehmigungen
  - Link zum Anzeigen des Managers

- Supportinformationen
- Attributzuordnung

  Ordnen Sie Attribute im Benutzerspeicher den Attributen zu, die in der mobilen App angezeigt werden.

Gehen Sie wie folgt vor:

1. Melden Sie sich in der Benutzerkonsole als Benutzer an, der die mobilen Konfigurationsaufgaben verwenden kann.
2. Klicken Sie auf "System", "Mobile Konfiguration", "Mobile Konfiguration erstellen".
3. Akzeptieren Sie die Standardoption "Neues Objekt des Typs 'Mobile Konfiguration' erstellen".
4. Füllen Sie die erforderlichen Felder auf der Registerkarte "Allgemein" aus. Sie können ein Bild für die mobile App angeben.

   Basis-URL

   Überprüfen Sie die Basis-URL der aktuellen Umgebung. Die Basis-URL wird automatisch aufgefüllt, wenn Sie eine mobile Konfiguration erstellen.

   CA IdentityMinder verwendet die Basis-URL, um den Servernamen, den Port und das Protokoll abzurufen, die die mobile App verwendet, um die URL für die REST-Aufrufe zu erstellen.

   Konfiguration

   Navigieren Sie zu einer Konfiguration, oder geben Sie einen eindeutigen Konfigurationsnamen ein.

   Version

   Vergrößern Sie die Versionsnummer, wenn Sie eine Konfiguration ändern und speichern.

   Die mobile App verwendet die Versionsnummer, um zu bestimmen, wann sie eine neue Version der Konfiguration herunterladen soll. Wenn die mobile App startet, dann wird die Versionsnummer des Servers mit der Version der geladenen Konfiguration verglichen. Wenn eine neue Version verfügbar ist, aktualisiert die mobile App die Konfiguration.

   Hinweis: Erhöhen Sie die Versionsnummer nicht, wenn Sie die Datei zum ersten Mal ändern.

   Branding-Image

   Geben Sie die volle URL einer PNG-Bilddatei mit einem transparenten Hintergrund an. Das Bild wird oben im Fenster der mobilen App angezeigt.
5. Wählen Sie auf der Registerkarte "Funktionen" die Funktionen für die mobile App aus.
6. Geben Sie auf der Registerkarte "Support" die Support-Informationen für mobile Benutzer an.

7. Ordnen Sie auf der Registerkarte "Attributzuordnung" Attribute der mobilen App zu Attributen im CA IdentityMinder-Benutzerspeicher zu. Sie können Attribute zu physischen oder bekannten Attributen zuordnen.
8. Geben Sie auf der Registerkarte "Zusätzliche Eigenschaften" zusätzliche Eigenschaftswertpaare an, um neue Funktionen oder Felder in der mobilen App zu unterstützen.

   Verwenden Sie folgendes Format:

   Key1=value1

   Key2=value2

   Key3=value3

   Hinweis: CA Technologies stellt Anweisungen bereit, wenn Administratoren zusätzliche Eigenschaften hinzufügen müssen. In dieser Version müssen Sie keine zusätzlichen Eigenschaften angeben.
9. Geben Sie auf der Registerkarte "Mitglieder" Regeln an, die die Auswahl der Benutzer festlegt, denen diese Konfiguration auf der mobilen App angezeigt wird.
10. Klicken Sie auf "Senden".

Download der mobilen App

Sobald die mobile App konfiguriert ist, können Endbenutzer sie im Apple Store herunterladen. Um die mobile App im Apple Store zu finden, suchen Sie nach "CA IdentityMinder".

Der Endbenutzer kann dann sein Gerät registrieren, wie z. B. ein Smartphone oder ein Tablet, indem die Anweisungen und der Code verwendet werden, die in der E-Mail enthalten sind.

Fehlerbehebung bei mobilen Apps

Wenn bei einem Benutzer ein Problem mit der mobilen App auftritt, können Supporttechniker eine Protokolldatei anfordern, um den Benutzer bei der Fehlerbehebung zu unterstützen.

Der mobile Benutzer aktiviert die Fehlerbehebung über das iPhone oder iPad. Nachdem die Fehlerbehebung aktiviert wurde, kann der mobile Benutzer die mobile App verwenden, um das Protokoll an eine E-Mail-Adresse des Supports zu senden.

Um das Generieren von Protokollen auf der mobilen App zu aktivieren, führt der mobile Benutzer die folgenden Schritte aus.

1. Navigieren Sie auf dem iPhone oder iPad zu "Einstellungen", "IdentityMinder", "Debug".
2. Klicken Sie auf "Aktiviert".
3. Starten Sie die Anwendung neu, und führen Sie die Aktionen aus, die im Protokoll angezeigt werden sollen.
4. Klicken Sie auf der Registerkarte "Hilfe" der mobilen CA IdentityMinder-App auf "Email Log" (E-Mail-Protokoll).

   Die mobile App erstellt eine E-Mail mit angehängter Protokolldatei. Die E-Mail wird an die in der Benutzerkonsole für den Support eingerichtete E-Mail-Adresse gesendet.

Kapitel 18: CA Berichte zu Benutzeraktivitäten

Dieses Kapitel enthält folgende Themen:

CA Enterprise Log Manager-Funktionen (siehe Seite 541)
Integrieren von zusätzlichen CA Enterprise Log Manager-Berichten oder -Abfragen mit CA Identity Manager (siehe Seite 553)

CA Enterprise Log Manager-Funktionen

Wenn CA Enterprise Log Manager mit CA Identity Manager integriert wird, stehen die folgenden Funktionen zur Verfügung:

- Der CA Enterprise Log Manager-Agent erfasst CA Identity Manager-Audit-Informationen und sendet diese an CA Enterprise Log Manager, damit sie in die CA ELM-Schemadefinition konvertiert werden.
- Die CA IdentityMinder-Benutzerkonsole kann CA Enterprise Log Manager-Berichte und/oder -Abfragen mit CA Identity Manager-Kontextinformationen, die zum Filtern der zurückgegebenen Informationen verwendet werden, nahtlos abrufen.
- CA Identity Manager umfasst mehrere Standardberichte und die Infrastruktur zum Hinzufügen von CA Enterprise Log Manager-Berichten und/oder -Abfragen zu einer vorhandenen oder neuen Aufgabe.
- CA Enterprise Log Manager Agent ist auf dem CA Identity Manager-Rechner [Audit-Datenbank] installiert
- CA Identity Manager Connector wird für CA Enterprise Log Manager Agent konfiguriert
- CA Enterprise Log Manager-Produktregistrierung wird für die Identity Manager-Umgebung erstellt
- Optionaler CA Enterprise Log Manager-Datenzugriffsfilter wird für die Produktregistrierung erstellt

CA Enterprise Log Manager-Komponenten

Wenn CA IdentityMinder mit CA Enterprise Log Manager integriert wird, werden die folgenden Komponenten zur CA IdentityMinder-Architektur hinzugefügt:

- Auf der CA ELM-Viewer-Registerkarte können Sie CA Enterprise Log Manager-Objekte in eine neue oder vorhandene Aufgabe einbetten.

  Hinweis: Dafür muss eine CA Enterprise Log Manager-Serververbindung konfiguriert sein.

- Rollendefinitionen, die importiert werden können

Beschränkungen bei der Integration

Folgende Beschränkungen sind bei der Integration des Frameworks mit dem CA Enterprise Log Manager-Server bekannt:

- Zur Laufzeit werden Abfrage- und Berichtlisten für die Aufgabenkonfiguration möglicherweise nur langsam abgerufen.
- Die CA Enterprise Log Manager-APIs erkennen nur Zeitzonen mit standardmäßigen Java-Benennungen.
- Bei der Operation EQUAL wird die Groß- und Kleinschreibung berücksichtigt, wenn sie in einem zusammengesetzten Filter verwendet wird.
- Die minimal zulässige Version für den CA Enterprise Log Manager-Server ist der CA ELM-Server (45.10) mit den folgenden in der angezeigten Reihenfolge durchgeführten automatischen Software-Updates:

  1. Automatischer Software-Patch SP-1
  2. Inhalts-Patch M5
  3. Update für offene API

- Es wird immer nur eine Verbindung mit einem CA Enterprise Log Manager-Server unterstützt.

Integrieren von CA Enterprise Log Manager mit CA IdentityMinder

Damit CA Enterprise Log Manager-Berichte und -Abfragen angezeigt und verwaltet werden können, muss der Administrator Folgendes durchführen:

1. Installieren des CA Enterprise Log Manager-Agenten
2. Erstellen Sie einen neuen Connector.
3. Aktivieren Sie die Überprüfung in CA IdentityMinder.
4. Konfigurieren des CA Enterprise Log Manager-Servers

Installationsvoraussetzungen für den CA Enterprise Log Manager-Agenten

Folgendes muss durchgeführt werden, bevor der CA Enterprise Log Manager-Agent installiert wird:

- Vergewissern Sie sich, dass Sie von dem Rechner, auf dem CA IdentityMinder ausgeführt oder die CA IdentityMinder-Überprüfungsdatenbank gehostet wird, auf den CA Enterprise Log Manager-Serverrechner zugreifen können.
- Vergewissern Sie sich, dass Sie vom Serverrechner auf den Agent-Rechner zugreifen können.
- Konfigurieren Sie die Datenquelle auf dem Agentenrechner. Klicken Sie hier (siehe Seite 543), um Anweisungen zu erhalten.
- Überprüfen Sie, ob Adobe Flash Player in der Version 9.0.28 oder höher installiert ist. Sie können den Player von hier herunterladen:

  http://www.adobe.com/go/getflash
- Laden Sie Binärdateien des Agenten herunter Klicken Sie hier (siehe Seite 544), um Anweisungen zu erhalten.
- Ermitteln Sie den Authentifizierungsschlüssel des Agenten. Klicken Sie hier (siehe Seite 544), um Anweisungen zu erhalten.
- Ermöglichen des einfachen Zugriffs auf den Servernamen/die Server-IP
- Ermöglichen Sie einfachen Zugriff auf Kontoinformationen, ohne die Sicherheit zu gefährden. Dies ist das Identitätskonto, unter dem der Agent als Service ausgeführt wird (Windows).
- Wenn der Connector bereits vorhanden ist, exportieren Sie die Connector-Standardinformationen, sodass diese schnell verfügbar sind.
- Vergewissern Sie sich, dass auf dem Rechner 4 GB RAM verfügbar sind.

Konfigurieren der Datenquelle auf dem Agentenrechner

Gehen Sie folgendermaßen vor, um die Datenquelle auf dem Agentenrechner zu konfigurieren.

So konfigurieren Sie die Datenquelle

1. Navigieren Sie zu "Systemsteuerung", "Verwaltung", "Datenquellen (ODBC)".
2. Fügen Sie auf der Registerkarte "System-DSN" Folgendes hinzu:

   imsauditevent12 Datenquelle (ODBC) - die auf die Überprüfungsdatenbank zeigt.
3. Klicken Sie auf "Übernehmen"/"OK".

   Die Datenquelle ist konfiguriert.

Herunterladen der Binärdateien des Agenten

Gehen Sie folgendermaßen vor, um Binärdateien des Agenten herunterzuladen.

So laden Sie Binärdateien des Agenten herunter:

1. Melden Sie sich beim CA Enterprise Log Manager-Server mit der folgenden URL an:

   https://<Host>:5250/spin/calm/CALMSpindle.csp

2. Navigieren Sie zu "Verwaltung", "Protokollerfassung", "Agenten-Explorer", "Binärdateien des Agenten herunterladen", "<OS> <version>"

3. In Datei speichern.

Abrufen des Authentifizierungsschlüssels des Agenten

Gehen Sie folgendermaßen vor, um den Authentifizierungsschlüssel des Agenten abzurufen.

So rufen Sie den Authentifizierungsschlüssel des Agenten ab

1. Navigieren Sie auf dem CA Enterprise Log Manager-Server zu "Verwaltung", "Protokollerfassung", "Agenten-Explorer", "Authentifizierungsschlüssel des Agenten".

2. Ermöglichen Sie einfachen Zugriff auf den Schlüssel, ohne die Sicherheit zu gefährden.

Installieren des CA Enterprise Log Manager-Agenten

Der CA Enterprise Log Manager-Agent ist dafür zuständig, Ereignisse zu erfassen und diese Informationen zum CA Enterprise Log Manager-Server zu senden. Installieren Sie den Agenten auf einem CA IdentityMinder-Datenbankserver oder -Endpunktrechner, um die Protokollierung zu ermöglichen.

Hinweis: Der CA Enterprise Log Manager-Agent wird unter Windows und Linux unterstützt.

So installieren Sie den CA Enterprise Log Manager-Agenten

1. Führen Sie auf dem Datenbankserver die Installation mit der ca-elmagent-<Version>.exe-Datei aus, und geben Sie das Folgende an:

   Name/IP-Adresse des CA Enterprise Log Manager-Servers und den Authentifizierungscode.

   Agent-Server-Kontoinformationen, die zur Ausführung des Agenten als Service/Dämon verwendet werden sollen.

2. Geben Sie die Standard-Connector-Listendatei an, wenn verfügbar.
3. Melden Sie sich beim CA Enterprise Log Manager-Server mit der folgenden URL an:

   https://<Host> :5250/spin/calm/CALMSpindle.csp

4. Navigieren Sie zu "Verwaltung", "Protokollerfassung", "Agenten-Explorer", Standardagentengruppe
5. Wählen Sie den Agentenrechner aus, und starten Sie die Ansicht "Status und Befehl".

   Der Statusprozess sollte ausgeführt werden.

Importieren von Rollendefinitionen

Um die Enterprise Log Manager-Verbindung in der Benutzerkonsole konfigurieren zu können, müssen Sie zunächst die CA Enterprise-Rollendefinitionen importieren.

So importieren Sie die Rollendefinitionen:

1. Melden Sie sich bei der Management-Konsole über die folgende URL an.

   `http://Host:Port/iam/immanage`

2. Navigieren Sie zu "Umgebung", "Role and Task Settings" (Rollen- und Aufgabeneinstellungen). Klicken Sie auf die Schaltfläche "Importieren", und wählen Sie "Enterprise Log Manager - Enterprise Log Manager Role Definitions.xml" aus.
3. Klicken Sie auf "Speichern und schließen".
4. Klicken Sie auf der Registerkarte "System" in der Benutzerkonsole auf "Enterprise Log Manager-Verbindung konfigurieren", geben Sie die erforderlichen Informationen ein, und klicken Sie auf "Senden".

Erstellen eines neuen Connector

Gehen Sie folgendermaßen vor, um einen neuen Connector zu erstellen.

So erstellen Sie einen neuen Connector

1. Melden Sie sich beim CA Enterprise Log Manager-Server mit der folgenden URL an:

   `https://<Host> :5250/spin/calm/CALMSpindle.csp`

2. Navigieren Sie zu "Verwaltung", "Protokollerfassung", "Agenten-Explorer", Standardagentengruppe
3. Wählen Sie den Agentenrechner aus.
4. Wechseln Sie zur Ansicht "Connectors".
5. Klicken Sie auf die Schaltfläche "Neuen Connector erstellen", und geben Sie die folgenden Informationen ein:

   Connector-Details

   Wählen Sie als Integrationstyp "CAIdentityManager" aus, und ändern Sie ggf. den Connector-Namen.

   Connector-Konfiguration

   Verbindungszeichenfolge

   - Driver={SQL Server} ; Server=<Audit-DB-Server> ; Database=<Audit-DB>
   - Driver={Microsoft ODBC for Oracle} ; Dbq=<Audit-DB-TNSname>

   Benutzername: <Audit-DB-Benutzer>

   Kennwort: <Überwachungs-DB-Benutzerkennwort>

6. Übernehmen Sie die folgenden Änderungen der Verbindungskonfiguration für den CA Identity Manager Connector zur Verwendung mit 12.6.3.
   - SourceName: der Datenquellen-Name auf dem Agentrechner - imsauditevent12
   - AnchorSQL: max(id) aus imsauditevent12 auswählen
   - AnchorField: IMS_EVENTID
   - EventSQL:

     ```
     select imsauditevent12.id as IMS_EVENtid ,imsauditevent12.audit_time as
     IMS_AUDITTIME ,imsauditevent12.envname as ENVNAME
     ,imsauditevent12.admin_name as ADMINUNIQUENAME ,imsauditevent12.admin_dn as
     ADMINID ,imsauditevent12.tasksession_oid as TRANSACTIONID
     ,imsauditevent12.event_description as EVENTINFO
     ,imsauditevent12.event_state as EVENTSTATE
     ,imsauditevent12.tasksession_oid as TASKOID
     ,imsauditttasksession12.task_name as TASKNAME
     ,imsauditeventobject12.object_type as OBJECTTYPE ,
     imsauditeventobject12.object_name as
     ```

```
OBJECTUNIQUENAME ,imsauditobjectattributes12.attribute_name as ATTRNAME
,imsauditobjectattributes12.attribute_oldvalue as ATTROLDVALUE
,imsauditobjectattributes12.attribute_newvalue as ATTRNEWVALUE
,imsauditobjectattributes12.attribute_newvalue as ATTRVALUE from
imsauditTasksession12, imsauditevent12, imsauditeventobject12,
imsauditobjectattributes12 where imsauditevent12.id >? and
imsauditevent12.tasksession_id = imsauditTasksession12.id and
imsauditevent12.tasksession_oid = imsauditTasksession12.tasksession_oid
and
imsauditeventobject12.parent_event_id = imsauditevent12.id and
imsauditobjectattributes12.parent_object_id = imsauditeventobject12.id
ORDER BY
imsauditevent12.id ASC;
```

7. Klicken Sie auf "Speichern und schließen".

So überprüfen Sie, dass der Connector funktioniert

1. Navigieren Sie zu "Verwaltung", "Protokollerfassung", "Agenten-Explorer", Standardagentengruppe
2. Wählen Sie den Agentenrechner aus.
3. Wechseln Sie zur Ansicht "Connectors", und klicken Sie auf die Schaltfläche "Launch Status and Command View" (Status- und Befehlsansicht starten).

   Der Statusprozess sollte ausgeführt werden.

Aktivieren der Überwachung in CA Identity Manager

So aktivieren Sie die Überwachung in CA Identity Manager

1. Öffnen der Verwaltungskonsole

   `http://Host:Port//iam/immanage`

2. Navigieren Sie zu "Environments" (Umgebungen), <Umgebung>, "Advanced Setting" (Erweiterte Einstellung), "Auditing" (Überprüfung).
3. Exportieren Sie vorhandene Einstellungen, und speichern Sie die Datei.
4. Ändern Sie die gespeicherte Datei folgendermaßen, und speichern Sie die Änderungen:
   - <Audit enabled="true" auditlevel="BOTH" datasource="auditDbDataSource"
   - Fügen Sie das Überwachungsprofil für Kennwortrichtlinien unter dem letzten bereits definierten Überwachungsprofil hinzu:

     <AuditProfile objecttype="FWPASSWORDPOLICY" auditlevel="BOTHCHANGED"/>
5. Importieren Sie die Datei zurück in die Management-Konsole, und verwenden Sie eine der folgenden Optionen, um die Aggregation von Überprüfungsinformationen auszulösen:
   - Aufgaben, die für ein auf Benutzerebene verwaltetes Objekt ausgeführt werden
   - Aufgaben, die für ein auf Gruppenebene verwaltetes Objekt ausgeführt werden
   - Aufgaben, die für ein auf Ebene der Kennwortrichtlinien verwaltetes Objekt ausgeführt werden
6. Melden Sie sich beim CA Enterprise Log Manager-Server mit der folgenden URL an:

   https://<Host> : 5250/spin/calm/CALMSpindle.csp
7. Um vorhandene Berichte auszuführen, navigieren Sie zu "Abfragen und Berichte", "Abfragen", "CA Identity Manager".

   Hinweis: Der Enterprise Log Manager-Server muss bereits konfiguriert sein.
8. Öffnen Sie, je nach den Aufgaben, die Sie ausgeführt haben, die folgenden Standardberichte, um zu überprüfen, dass Ereignisse erzeugt werden:
   - Die Aufgabe "Alle Ereignisse des Systems nach Benutzer" startet "CA Identity Manager - Alle Ereignisse des Systems" gefiltert nach der Benutzer-ID.
   - Die Aufgabe "Kontoverwaltung nach Host" startet "Kontoverwaltung nach Host" ohne Änderung.
   - Die Aufgabe "Kontoerstellungen nach Konto" startet "Kontoerstellungen nach Konto" ohne Änderung.
   - Die Aufgabe "Kontolöschungen nach Konto" startet "Kontolöschungen nach Konto" ohne Änderung.

- Die Aufgabe "Kontosperrungen nach Konto" startet "Kontosperrungen nach Konto" ohne Änderung.
- Die Aufgabe "Zertifizierungsprozess nach Host" startet "CA Identity Manager - Prozessaktivität nach Host" ohne Änderung.
- Die Aufgabe "Kennwortrichtlinienänderung" startet "CA Identity Manager - Richtlinienänderungen" ohne Änderung.

Konfigurieren des CA Enterprise Log Manager-Servers

Bevor Sie den CA Enterprise Log Manager-Server für die Verwaltung konfigurieren, überprüfen Sie Folgendes:

- Sie müssen über "EiamAdmin"-Anmeldeinformationen verfügen.
- Adobe Flash Player Version 9.0.28 oder höher muss installiert sein.

Nachdem der CA Enterprise Log Manager-Server konfiguriert wurde, sind die folgenden Funktionen verfügbar:

- Mehrere Umgebungen, die Überwachungsereignisse erzeugen, werden von einem einzelnen CA Enterprise Log Manager-Server oder einer föderierten Hierarchie belegt.
- Die Datenautorisierung für Remote-Systeme kann über den Datenzugriffsfilter des CA Enterprise Log Managers implementiert werden.

So konfigurieren Sie den CA Enterprise Log Manager-Server

1. Melden Sie sich auf der Produktregistrierungsseite des CA Enterprise Log Manager-Servers mit den Administrator-Anmeldeinformationen für CA Enterprise Log Manager über die folgende URL an:

   `https://Host:Port/spin/calmapi/products.csp`

2. Registrieren Sie Ihre CA IdentityMinder-Umgebung, indem Sie auf die Schaltfläche "Registrieren" klicken und den Zertifikatsnamen und das Kennwort angeben.

   Hinweis: Jede Umgebung erfordert ein separates Registrierungspaar (Zertifikatsname/Kennwort).

3. Navigieren Sie zu "Verwaltung", "Benutzer- und Zugriffsverwaltung", "New Data Access Filter" (Neuer Datenzugriffsfilter), und geben Sie einen Namen für den zu erstellenden Filter an.
4. Fahren Sie mit dem nächsten Schritt fort.
5. Behalten Sie für "Ausgewählte Identitäten" die Angabe "Alle Identitäten" bei, und fahren Sie mit dem nächsten Schritt fort.
6. Erstellen Sie einen Zugriffsfilter, indem Sie auf die Schaltfläche "Neuer Ereignisfilter" klicken.

   Konfigurieren Sie den Datenzugriffsfilter, indem Sie das Zertifikat auf den Rechner/Umgebungsnamen für Protokolle beschränken, die von CA IdentityMinder erfasst wurden. Sie können das Zertifikat auch auf den ausschließlichen Zugriff auf systemeigene Endpunktinformationen für verwaltete Endpunkte beschränken.

7. Klicken Sie auf "Speichern und schließen".
8. Öffnen Sie die Zugriffsrichtlinien, indem Sie auf die Schaltfläche "Open Access Policies" (Zugriffsrichtlinien öffnen) klicken.
9. Wählen Sie "Obligation Policies" (Verbindliche Richtlinien) aus, und klicken Sie auf die verfügbare Richtlinie.

10. Entfernen Sie die Angabe "Alle Identitäten", und fügen Sie den Zertifikatsnamen hinzu.
11. Speichern Sie die Richtlinie.
12. Melden Sie sich bei der Identity Manager-Benutzerkonsole an, und konfigurieren Sie die Enterprise Log Management-Verbindung.

Konfigurieren der Enterprise Log Manager-Verbindung

Sie verwalten neu hinzugefügte CA Enterprise Log Manager-Verbindungsaufgaben in diesem Fenster.

Dieses Fenster enthält folgende Felder:

Verbindungsname

Legt den eindeutigen Namen fest, der für das einzelne verwaltete CA ELM-Verbindungsobjekt verwendet wird.

Dieses Feld ist schreibgeschützt.

Beschreibung

Beschreibt die CA ELM-Verbindung.

Hostname

Legt den Hostnamen oder die IP-Adresse des CA Enterprise Log Manager-Servers fest.

Dieses Feld ist erforderlich.

Port-Nr.

Legt den Verbindungs-Port für dne CA Enterprise Log Manager-Server fest.

Standard: 52520

Dieses Feld ist erforderlich.

Von einer Zertifizierungsstelle unterzeichnetes SSL-Zertifikat

Wenn dieses Kontrollkästchen aktiviert ist, wird eine strikte SSL-Zertifikatsprüfung bei der Herstellung einer Verbindung mit einem CA Enterprise Log Manager durchgeführt.

Wenn Sie über ein selbst signiertes SSL-Zertifikat verfügen, z. B. ein standardmäßig mit CA Enterprise Log Manager installiertes Zertifikat, darf dieses Kontrollkästchen nicht aktiviert werden, da kein vertrauenswürdiger Pfad zur Root Certificate Authority vorhanden ist.

Zertifikatsname

Legt den Namen des für die Authentifizierung zu verwendenden CA Enterprise Log Manager-Zertifikats fest.

Dieses Feld ist erforderlich.

Zertifizierungskennwort

Legt das CA Enterprise Log Manager-Kennwort fest.

Dieses Feld ist erforderlich.

Attribut

Nicht unterstützt. Die Version wird abgerufen, wenn das Speichern von Verbindungsinformationen versucht wird.

Löschen der Enterprise Log Manager-Verbindung

Wählen Sie eine Verbindung aus der Liste aus, und klicken Sie auf "Löschen". Die CA Enterprise Log Manager-Verbindungsaufgabe wird gelöscht.

Integrieren von zusätzlichen CA Enterprise Log Manager-Berichten oder -Abfragen mit CA Identity Manager

Sie können zusätzliche CA Enterprise Log Manager-Berichte oder -Abfragen mit CA Identity Manager über die Enterprise Log Manager-Viewer-Registerkarte integrieren. Diese neuen Berichte oder Abfragen können mit vorhandenen Aufgaben (einschließlich Assistenten) und neuen Aufgaben verbunden werden. Föderierte Daten von CA Enterprise Log Manager können bei Bedarf auch eingeschlossen werden. Über die Enterprise Log Manager-Viewer-Registerkarte können Sie Filter auf die abgerufenen Informationen anwenden. Für diese Filter kann Folgendes verwendet werden:

- Konstante Werte
- Attribute des verwalteten Objekts
  - Zum Beispiel: physisch - ::MyPhysicalAttribute::

    logisch - ::|MyLogicalAttribute|::
- Jedes Feld, wie in der CA ELM-Schemadefinition (CEG) beschrieben
  - dest_username
  - dest_objectname
  - dest_uid
  - source_username
  - source_objectname
  - source_uid
  - ...

Registerkarte "Konfigurieren der Enterprise Log Manager-Viewer"

Konfigurieren Sie die "CA Enterprise Log Manager"-Registerkarte so, dass sie mit einem beliebigen oder mit allen der folgenden Felder angezeigt wird:

Name

Ein Name, den Sie der Registerkarte zuweisen.

Tag

Eine ID für die Registerkarte, die innerhalb dieser Aufgabe eindeutig ist. Sie muss mit einem Buchstaben oder Unterstrich beginnen und darf nur Buchstaben, Zahlen oder Unterstriche enthalten. Der Tag wird hauptsächlich zum Festlegen von Datenwerten durch XML-Dokumente oder HTTP-Parameter verwendet.

Registerkarte ausblenden

Verhindert, dass die Registerkarte in der Aufgabe sichtbar ist. Diese Option ist für Anwendungen praktisch, bei denen die Registerkarte zwar ausgeblendet werden soll, der Zugriff auf die Attribute auf der Registerkarte jedoch weiterhin möglich sein soll.

Enterprise Log Manager-Abfrage

Legt fest, dass CA Enterprise Log Manager-Abfragen angezeigt werden sollen.

Hinweis: Sie können entweder CA Enterprise Log Manager-Abfrage oder CA Enterprise Log Manager-Bericht festlegen, aber nicht beide.

Enterprise Log Manager-Bericht

Legt fest, dass CA Enterprise Log Manager-Berichte angezeigt werden sollen.

Hinweis: Sie können entweder CA Enterprise Log Manager-Abfrage oder CA Enterprise Log Manager-Bericht festlegen, aber nicht beide.

Enterprise Log Manager-Id

Gibt die ID entweder für die Abfrage oder den Bericht an.

Föderierte Daten einschließen

Schließt föderierte Daten von CA Enterprise Log Manager in den Ergebnissen ein oder aus. Dieses Feld ist standardmäßig aktiviert.

Eingabeaufforderung anzeigen

Gibt nur Eingabeaufforderungen von CA Enterprise Log Manager-Abfragen an. Dieses Feld ist standardmäßig aktiviert.

Filter

Gibt erweiterte SQL-basierte Bedingungen an, die zur Eingrenzung der Ergebnisse von CA Enterprise Log Manager-Abfragen oder -Berichten verwendet werden. Konstante und dynamische Werte können enthalten sein. Im Folgenden ist ein Beispielausdruck dargestellt.

```
((source_uid EQUAL ::logical.attribute.X:: ) AND (source_username EQUAL
::logical.attribute.Y:: ))
```

Zu den unterstützten Vorgängen gehören:

- gleich (EQUAL)
- ungleich (NEQ)
- kleiner (LESS)
- größer (GREATER)
- kleiner gleich (LEQ)
- größer gleich (GREATEQ)
- wie (LIKE)
- nicht wie (NOTLIKE)
- in Gruppe (INSET)
- nicht in Gruppe (NOTINSET)

Zu den unterstützten Operatoren gehören:

- AND
- OR

Klammern sind obligatorisch. Wenn der Wert auf der linken Seite im Bedingungsausdruck nicht die Markierung "::" an beiden Enden aufweist, wird der Wert als Konstante betrachtet und entsprechend an den CA Enterprise Log Manager gesendet.

Tabelle "Parameter/Wert"

Gibt für Scoping zu verwendende Felder und Werte an.

Nur mit Tags übereinstimmende Abfragen oder Berichte und Tags-Logik des Scoping werden ausgewählt.

Parameter

Gibt die Werte für die Start-, Stop- und Limit-Parameter an. Folgende Parameter werden unterstützt:

- Zeitgranularität (nur für Trends)
- Startzeit
- Endzeit
- Frühestes gruppiertes Ereignis besitzt Datum nach (nur für gruppierte Abfragen)
- Spätestes gruppiertes Ereignis besitzt Datum nach (nur für gruppierte Abfragen)
- Spätestes gruppiertes Ereignis besitzt Datum vor (nur für gruppierte Abfragen)

- Die minimale Anzahl von Ereignissen in der Gruppierung (nur für gruppierte Abfragen)
- Die maximale Anzahl von Ereignissen in der Gruppierung (nur für gruppierte Abfragen)

Kapitel 19: Zugriffsrollen

Zugriffsrollen bieten eine zusätzliche Möglichkeit, Berechtigungen in CA IdentityMinder oder einer anderen Anwendung anzugeben. Sie können Zugriffsrollen z. B. für Folgendes verwenden:

- Angeben von indirektem Zugriff auf ein Benutzerattribut
- Erstellen komplexer Ausdrücke
- Festlegen eines Attributs in einem Benutzerprofil, das von einer anderen Anwendung verwendet wird, um Berechtigungen zu bestimmen

Zugriffsrollen sind insofern ähnlich zu Identitätsrichtlinien, als sie einen Satz von Geschäftsänderungen auf einen Benutzer oder eine Gruppe von Benutzern anwenden. Wenn Sie eine Zugriffsrolle verwenden, um Geschäftsänderungen anzuwenden, können Sie jedoch feststellen, auf welche Benutzer sich die Änderungen beziehen, indem Sie die Mitglieder der Zugriffsrolle anzeigen.

In den meisten Fällen werden Zugriffsrollen nicht zu Aufgaben zugeordnet.

Hinweis: Wenn CA IdentityMinder mit CA SiteMinder integriert ist, können Zugriffsrollen auch Zugriff auf Anwendungen ermöglichen, die von CA SiteMinder geschützt werden. In diesem Fall schließen Zugriffsrollen Zugriffsaufgaben ein. Weitere Informationen finden Sie im Kapitel zur SiteMinder-Integration im *Konfigurationshandbuch*.

Dieses Kapitel enthält folgende Themen:

So verwalten Zugriffsrollen Berechtigungen (siehe Seite 558)
Beispiel: Indirekte Änderung eines Profilattributs (siehe Seite 558)
Erstellen einer Zugriffsrolle (siehe Seite 559)

So verwalten Zugriffsrollen Berechtigungen

Sie können Zugriffsrollen verwenden, um Berechtigungen zu verwalten, indem Sie Änderungsaktionen angeben, die auftreten, wenn ein Benutzer hinzugefügt oder als ein Mitglied oder Administrator einer Rolle entfernt wird.

Um Zugriffsrollen zu verwenden, führen Sie die folgenden Schritte aus:

1. Ein Administrator erstellt eine Zugriffsrolle.
2. Auf der Registerkarte "Mitglieder" gibt der Administrator Hinzufügungs- oder Entfernungsaktionen an, die die Aktionen bestimmen, die CA IdentityMinder ausführt, wenn die Zugriffsrolle einem Benutzer zugewiesen ist.
3. Der Administrator gibt nach Bedarf Administrator- und Eigentümerrichtlinien an, und sendet die Aufgabe, um die Zugriffsrolle zu erstellen.
4. Administratoren von Zugriffsrollen weisen die Zugriffsrolle den Benutzern zu.
5. CA IdentityMinder stellt die in der Rolle angegebenen Hinzufügungsaktionen fertig.

Beispiel: Indirekte Änderung eines Profilattributs

Sie können Zugriffsrollen verwenden, um ein Attribut im Profil eines Benutzers indirekt zu ändern. Zum Beispiel will es ein Unternehmen möglicherweise keinem Benutzer erlauben, den Titel eines anderen Benutzers direkt zu ändern. Das Unternehmen kann eine Zugriffsrolle erstellen, die einen Titel ändert, wenn ein Administrator die Rolle einem Benutzer zuweist.

Um ein Attribut indirekt zu ändern, legen Sie die Änderungsaktionen für die Zugriffsrolle fest. Wenn ein Administrator die Rolle zuweist, kann die Änderungsaktion eine oder mehrere Änderungen an einem Attribut im Profil des Benutzers machen.

Um eine Zugriffsrolle dazu zu verwenden, ein Attribut indirekt zu ändern, gehen Sie wie folgt vor:

1. Erstellen Sie eine Zugriffsrolle.
2. Wählen Sie auf der Registerkarte "Mitglieder" das Kontrollkästchen "Administratoren können Mitglieder dieser Rolle hinzufügen oder aus ihr entfernen" aus und klicken Sie auf das Pfeilsymbol.

   CA IdentityMinder zeigt zusätzliche Felder für "Aktion hinzufügen" und "Aktion entfernen" an.
3. Wählen Sie in den Feldern "Aktion hinzufügen" oder "Aktion entfernen" eine Aktion aus dem Listenfeld aus.

   CA IdentityMinder zeigt zusätzliche Felder an, auf der Basis der Option, die Sie ausgewählt haben.

4. Konfigurieren Sie die Hinzufügungs- oder Entfernungsaktionen nach Bedarf.
5. Wählen Sie die Registerkarte "Administrator" aus, um die Administratoren anzugeben, die Mitglieder zur Zugriffsrolle hinzufügen können, die Sie erstellen.
6. Wählen Sie die Registerkarte "Eigentümer" aus, um die Administratoren anzugeben, die die Zugriffsrollendefinition ändern können.
7. Klicken Sie auf "Senden", um die Zugriffsrollenerstellung abzuschließen.
8. Weisen Sie nach Bedarf die Zugriffsrolle Benutzern zu.

Erstellen einer Zugriffsrolle

Das Erstellen einer Zugriffsrolle umfasst die folgenden Schritte:

- Beginnen Sie mit der Erstellung einer Zugriffsrolle (siehe Seite 559)
- Definieren des Profils für Zugriffsrollen (siehe Seite 560)
- Definieren von Mitgliederrichtlinien für Zugriffsrollen (siehe Seite 560)
- Definieren von Admin-Richtlinien für Zugriffsrollen (siehe Seite 561)
- Definieren von Eigentümerregeln für Zugriffsrollen (siehe Seite 561)

Beginnen Sie mit der Erstellung einer Zugriffsrolle

1. Melden Sie sich bei einem Identity Manager-Konto mit einer Rolle an, die eine Aufgabe zum Erstellen von Zugriffsrollen enthält.
2. Klicken Sie auf die Option "Zugriffsrollen" und dann auf die Option "Zugriffsrolle erstellen".

   Wählen Sie die Option aus, um eine neue Rolle oder eine Kopie einer Rolle zu erstellen. Wenn Sie die Option "Kopieren" auswählen, suchen Sie die Rolle.
3. Fahren Sie mit dem nächsten Abschnitt fort,Definieren des Profils für Zugriffsrollen.

Definieren des Profils für Zugriffsrollen

So definieren Sie das Profil für Zugriffsrollen:

1. Geben Sie einen Namen und eine Beschreibung ein, und vervollständigen Sie alle benutzerdefinierten Attribute, die für die Rolle definiert sind.

   Hinweis: Sie können auf dem Register "Profil" benutzerdefinierte Attribute angeben, die weitere Informationen zu Zugriffsrollen enthalten. Sie können diese zusätzlichen Informationen verwenden, um Rollensuchvorgänge in Umgebungen zu erleichtern, die eine große Anzahl von Rollen enthalten.

2. Wählen Sie die Option "Aktiviert" aus, wenn Sie die Rolle sofort nach der Erstellung für die Verwendung freigeben möchten.

3. Fahren Sie mit dem nächsten Abschnitt, Definieren von Mitgliederrichtlinien für Zugriffsrollen (siehe Seite 560), fort.

Definieren von Mitgliederrichtlinien für Zugriffsrollen

Führen Sie auf der Registerkarte "Mitglieder" die folgenden Schritte aus:

1. Wählen Sie die Option "Hinzufügen" aus, um die Mitgliederrichtlinien zu definieren.

2. (Optional) Definieren Sie auf der Seite "Mitgliederrichtlinie" eine Mitgliederregel im Hinblick darauf, wer diese Rolle verwenden darf.

   Dadurch weisen Sie die Rolle automatisch Benutzern zu, auf die die Kriterien in der Mitgliederrichtlinie zutreffen.

3. Verifizieren Sie, dass die Mitgliederrichtlinie auf der Registerkarte "Mitglieder" angezeigt wird.

   Klicken Sie auf das Pfeilsymbol auf der linken Seite, um eine Richtlinie zu bearbeiten. Klicken Sie auf das Symbol mit dem Minuszeichen, um sie zu entfernen.

4. Aktivieren Sie auf der Registerkarte "Mitglieder" das Kontrollkästchen "Administratoren können Mitglieder dieser Rolle hinzufügen oder entfernen".

   Nachdem Sie diese Funktion aktiviert haben, definieren Sie die Aktion "Hinzufügen" und die Aktion "Entfernen". Diese Aktionen definieren, was geschieht, wenn ein Benutzer als Mitglied der Rolle hinzugefügt oder entfernt wird.

5. Fahren Sie mit dem nächsten Abschnitt fort, Definieren von Admin-Richtlinien für Zugriffsrollen (siehe Seite 561).

Definieren Sie Admin-Richtlinien für Zugriffsrollen

Führen Sie auf der Registerkarte "Administratoren" die folgenden Schritte aus:

1. Wenn Sie die Option "Administratoren verwalten" verfügbar machen möchten, aktivieren Sie das Kontrollkästchen "Administratoren können Administratoren der Rolle hinzufügen und entfernen".

   Nachdem Sie diese Funktion aktiviert haben, definieren Sie die Aktionen, die ausgeführt werden sollen, wenn ein Benutzer als Administrator der Rolle hinzugefügt oder entfernt wird.

2. Fügen Sie auf der Registerkarte "Administratoren" Admin-Richtlinien hinzu, die Admin- und Bereichsregeln und Administratorberechtigungen enthalten. Jede Richtlinie erfordert zumindest eine Berechtigung ("Mitglieder verwalten" oder "Administratoren verwalten").

   Sie können mehrere Admin-Richtlinien mit verschiedenen Regeln und verschiedenen Berechtigungen für Administratoren hinzufügen, die die Regel erfüllen.

3. Klicken Sie auf das Pfeilsymbol auf der linken Seite, um eine Richtlinie zu bearbeiten. Klicken Sie auf das Symbol mit dem Minuszeichen, um sie zu entfernen.

4. Fahren Sie mit dem nächsten Abschnitt fort, Definieren von Eigentümerregeln für Zugriffsrollen (siehe Seite 561).

Definieren von Eigentümerregeln für Zugriffsrollen

Führen Sie auf der Registerkarte "Eigentümer" folgende Schritte aus:

1. Definieren Sie Eigentümerregeln, die bestimmen, welche Benutzer die Rolle ändern können.

2. Klicken Sie auf "Senden".

   Es wird eine Meldung mit der Information angezeigt, dass die Aufgabe gesendet wurde. Bevor Benutzer die Rolle verwenden können, kann es zu einer geringfügigen Verzögerung kommen.

Kapitel 20: Systemaufgaben

Dieses Kapitel enthält folgende Themen:

Standardsystemaufgaben (siehe Seite 563)
Hinzufügen von Benutzern mit einer Feeder-Datei (siehe Seite 564)
Registerkarte "Details der Loader-Datensätze" (siehe Seite 569)
Registerkarte "Zuordnung der Loader-Aktionen" (siehe Seite 570)
Registerkarte "Laderbenachrichtigungs-Details" (siehe Seite 571)
Bestätigen von Änderungen in der Massendatenlader-Aufgabe (siehe Seite 571)
Konfigurieren von E-Mail-Benachrichtigungen für Massendatenlader-Aufgaben (siehe Seite 573)
Planen der Aufgabe "Massendatenlader" (siehe Seite 573)
Ändern der Parser-Datei für den Massendatenlader (siehe Seite 573)
Webservice-Unterstützung für den Massendatenlader (siehe Seite 574)
JDBC-Verbindungsverwaltung (siehe Seite 575)
Logical-Attribute-Handler (siehe Seite 575)
Auswahlfelddaten (siehe Seite 579)
Aufgabenfenster "Korrelationsattribute konfigurieren" (siehe Seite 580)
Aufgabenfenster "Auf globaler Richtlinie basierter Workflow für Ereignisse konfigurieren" (siehe Seite 581)
Aufgabenstatus in CA IdentityMinder (siehe Seite 582)
Bereinigen gesendeter Aufgaben (siehe Seite 600)
Löschen wiederkehrender Aufgaben (siehe Seite 604)
Konfigurieren der Enterprise Log Manager-Verbindung (siehe Seite 605)
Löschen der Enterprise Log Manager-Verbindung (siehe Seite 606)
Geheime Schlüssel verwalten (siehe Seite 607)

Standardsystemaufgaben

CA IdentityMinder umfasst die folgenden Aufgaben, die Administratoren dabei unterstützen, eine CA IdentityMinder-Umgebung zu verwalten:

- Aufgaben des Typs "Gesendete Aufgaben anzeigen"

  Ermöglicht es Administratoren, den Status von Aufgaben in der Umgebung anzuzeigen. Entfernt auch veraltete Aufgaben aus der Ansicht "Gesendete Aufgaben anzeigen".

- Aufgaben des Typs "Massendatenlader"

  Lädt Feeder-Dateien hoch, die zum gleichzeitigen Bearbeiten vieler verwalteter Objekte verwendet werden.

- Massenaufgabe

  Ausführen einer Aufgabe für ein Objekt, z. B. einen Benutzer, basierend auf dessen Attributen, z. B. Abteilung, Stadt, Beendigungsdatum usw. Sie können diese Aufgabe regelmäßig ausführen, z. B. jeden Samstag.

  Sie können diese Aufgabe auch verwenden, um Massenänderungen an Benutzern vorzunehmen.

- Aufgaben des Typs "Auswahlfelddaten"

  Ermöglicht es Administratoren, Dateien hochzuladen, die zum Auffüllen von Optionen in Feldern (z. B. Auswahlfeldern) in Admin-Aufgaben verwendet werden.

- Aufgaben des Typs "Logical-Attribute-Handler"

  Ermöglicht es Administratoren, logische Attribute zu verwalten, die zum Anzeigen von Benutzerspeicherattributen (so genannten physischen Attributen) in einem vom Benutzer lesbaren Format in Aufgabenfenstern verwendet werden.

- Aufgaben des Typs "JDBC-Verbindungsverwaltung"

  Konfiguriert die Verbindungsdetails des Datenbankservers in CA IdentityMinder.

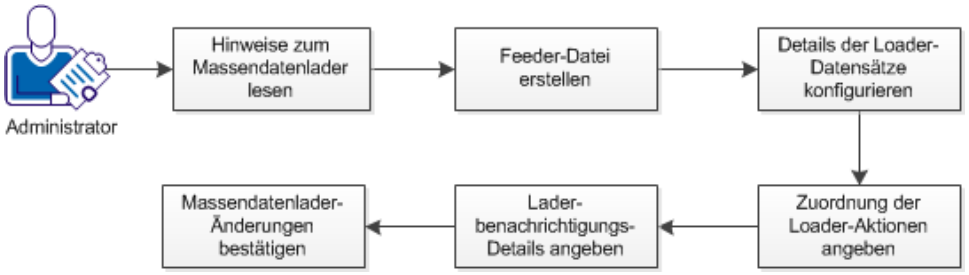
- E-Mail-Aufgaben

  Verwalten von E-Mail-Benachrichtigungsrichtlinien

Hinzufügen von Benutzern mit einer Feeder-Datei

Die Registerkarte "Massendatenlader" wird zum Hochladen von Feeder-Dateien verwendet, die zum gleichzeitigen Bearbeiten einer großen Anzahl an verwalteten Objekten verwendet wird. Sie können 1000 Benutzer im System beispielsweise manuell oder mit Hilfe des Massendatenladers erstellen. Die Massendatenlader-Aufgabe kann darüber hinaus einem Workflow-Prozess zugeordnet werden.

Der Massendatenlader-Client ist ein Befehlszeilenhilfsprogramm, das zur Batchverarbeitung dient. Wir empfehlen die Verwendung des Massendatenlader-Client, wenn (zum Zweck des Lastenausgleichs) Ihre Umgebung sich in einem Cluster befindet. Sie finden den Massendatenlader-Client auf dem Medium für die Bereitstellungskomponenten.



Gehen Sie wie folgt vor:

1. Überprüfen Sie die Hinweise zum Massendatenlader (siehe Seite 565).
2. Erstellen Sie eine CSV- oder XLS-Feeder-Datei (siehe Seite 568) und laden Sie sie hoch.
3. Konfigurieren Sie die Details der Loader-Datensätze (siehe Seite 569).

   Mit Hilfe dieser Registerkarte können Sie die Aktions- und die ID-Felder in der Feeder-Datei angeben.
4. Geben Sie die Zuordnung der Loader-Aktionen an (siehe Seite 570).

   In dieser Registerkarte können Sie das primäre Objekt auswählen und angeben, welche Aufgabe für die Aktion an einem Objekt ausgeführt werden soll.
5. Geben Sie die Laderbenachrichtigungs-Details an (siehe Seite 571).

   Diese Registerkarte ermöglicht es Ihnen, Benutzer auszuwählen, um Massendatenlader-Aufgabenänderungen zu bestätigen.
6. Bestätigen Sie und ändern Sie den Fortschritt der Massendatenlader-Aufgabenänderungen (siehe Seite 571).

Hinweise zum Massendatenlader

Die Registerkarte "Massendatenlader" wird zum Hochladen von Feeder-Dateien verwendet, die zum gleichzeitigen Bearbeiten einer großen Anzahl an verwalteten Objekten verwendet wird. Beachten Sie die folgenden Überlegungen bei der Verwendung des Massendatenladers:

- Achten Sie darauf, große Massenladungen zu ruhigen Zeiten zu planen, wie über Nacht. Große Massenladungen können sich auf die Leistung auswirken. In manchen Fällen kann eine Massenladung, die viele Unteraufgaben enthält, verhindern, dass von Benutzern gesendete Aufgaben abschließen, bis die Massenladung fertig ist.
- Wenn der Server während einer Aufgabe ausfällt, die viel Zeit in Anspruch nimmt (z. B das Hochladen einer großen Anzahl an Objekten), starten Sie von "Gesendete Aufgaben anzeigen" aus die Aufgabe neu. Beim Neustarten von Aufgaben wird nach dem letzten erfolgreich ausgeführten Datensatz begonnen.
- Falls Sie unter Solaris LDAP als Benutzerspeicher verwenden, kann es vorkommen, dass der Massendatenlader während des Importierens nicht reagiert. Um dieses Problem zu beheben, lesen Sie das Kapitel zur Angabe von LDAP-Verbindungseinstellungen im *Konfigurationshandbuch*. Nehmen Sie die dort aufgeführten Einstellungen vor.

- Wenn Sie mit Hilfe des Massendatenladers eine große Anzahl von Benutzern importieren, werden möglicherweise Ausnahmen angezeigt, dass der Arbeitsspeicher nicht ausreicht. Um dieses Problem zu lösen, stellen Sie die folgenden Speichergrößenparameter ein:
  - -Xmx
  - -XX:maxPermSize

    Hinweis: Weitere Informationen zur Feineinstellung von Speicherparametern finden Sie in Ihrer Anwendungsserverdokumentation.
- Wenn Sie den Bulk Loader verwenden, um viele verwaltete Objekte zu bearbeiten (wie Erstellung vieler Benutzer), kann sich dies auf die Leistung auswirken. Um die Leistung zu verbessern, beachten Sie die folgenden Empfehlungen:
  - Teilen Sie eine große CSV-Datei in mehrere kleine Dateien, wenn Sie die Benutzerkonsole für Massenladevorgänge verwenden. Beispiel: Zehn Massenladevorgänge von 10.000 Benutzern können schneller durchgeführt werden als ein Massenladevorgang von 100.000 Benutzern.

    Hinweis: EINE CSV-Datei mit mehr als 50.000 Einträgen kann Probleme im System verursachen.
  - Beschränken Sie die Anzahl der Aufgaben des Benutzers, der den Massenladevorgang durchführt. Beispiel: Die Leistung verbessert sich, wenn der Administrator, der den Massenladevorgang initiiert, nur ein paar Aufgaben hat. Wenn der Administrator viele Aufgaben hat, muss CA IdentityMinder umfassendere Berechtigungsprüfungen durchführen, die sich auf die Leistung auswirken können.
  - Beschränken Sie die Anzahl der Policy Xpress-Richtlinien, die mit den Massenänderungen verknüpft sind, die die Bereitstellung umfassen. Ziehen Sie auch in Betracht, einfache Policy Xpress-Richtlinien zu erstellen, die sich nicht in dem Maße auf die Leistung während eines Massenladevorgangs auswirken wie komplexe Richtlinien.
  - Überprüfen Sie, ob Sie über ausreichend Systemressourcen verfügen.

Beschränken der Datenvalidierung zur Leistungsverbesserung des Massendatenladers

Eine Admin-Aufgabe enthält normalerweise mehrere Registerkarten. Standardmäßig validieren Massenvorgänge Daten auf jeder Registerkarte in einer Aufgabe.

Validierung kann sich auf die Leistung von Massenvorgängen auswirken. Um die Leistung zu verbessern, können Sie die Datenvalidierung für Aufgabenregisterkarten deaktivieren, wenn keine Validierung erforderlich ist.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Benutzerkonsole als Benutzer an, der Änderungen von Admin-Aufgaben durchführen kann.
2. Wählen Sie die Option "Rollen und Aufgaben" und dann die Option "Admin-Aufgaben" aus. Wählen Sie dann die Option "Admin-Aufgaben ändern" aus.
3. Suchen Sie die Aufgabe, die für den Massenvorgang gilt, und wählen Sie die Aufgabe aus.
4. Wählen Sie "Registerkarten" aus, und wählen Sie anschließend die Registerkarte aus, die Sie ändern möchten.
5. Wählen Sie "Do Not Validate in Bulk Operations" (Nicht in Massenvorgängen validieren) aus, und klicken Sie dann auf "OK".
6. Wiederholen Sie die Schritte 4 und 5 für jede Registerkarte, für die keine Datenvalidierung erforderlich ist.
7. Klicken Sie auf "Senden".

   Datenvalidierung wird für die Registerkarten deaktiviert, die Sie geändert haben.

Beschränken von benutzerdefinierter Business-Logik

Auch die benutzerdefinierte Business-Logik, wie z. B. Business Logic-Task-Handler und Ereignis-Listener, in Aufgaben, die in Massenvorgängen verwendet werden, kann sich auf die Leistung auswirken.

Um die Leistung zu verbessern, deaktivieren Sie die benutzerdefinierte Business-Logik in Massenladungsvorgängen.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Managementkonsole.
2. Wählen Sie die anwendbare Umgebung aus, die den Ereignis-Listener oder den Business Logic-Task-Handler enthält.
3. Wählen Sie "Erweiterte Einstellungen", "Business Logic Task-Handler" (falls vorhanden) aus.

4. Legen Sie den Wert der Eigenschaft "UseInBulkOperation" auf "false" (falsch) fest, und klicken Sie dann auf "Speichern".
5. Wiederholen Sie Schritt 4 für Ereignis-Listener.
6. Sobald Sie die Änderungen für Business Logic-Task-Handler und Ereignis-Listener abgeschlossen haben, starten Sie die Umgebung neu.

Erstellen von Feeder-Dateien

Eine Massendatenladerdatei dient der Automatisierung wiederholt durchgeführter Aktionen, die für eine große Anzahl an verwalteten Objekten durchgeführt werden. Wenn Sie eine Feeder-Datei hochladen, analysiert das System die Feeder-Datei und liest sie.

Die Feeder-Datei muss die Dateierweiterung CSV oder XLS aufweisen und sollte die folgenden Eigenschaften aufweisen:

- Die Datei muss eine Kopfzeile enthalten, die die physischen Attribute, logischen Attribute oder bekannten Attributnamen eines verwalteten Objekts angibt.
- Die Header-Zeile muss eine Spalte enthalten, die die Aktion angibt, die für die Datensätze ausgeführt werden soll.
- Jede Zeile in einer Feeder-Datei wird als Datensatz bezeichnet. Die Datensätze enthalten die Werte für jedes der Attribute, die in der Header-Zeile angegeben sind. Folgende Optionen sind als Attributwerte zulässig:
  - Wert: Das Attribut wird auf den angegebenen Wert festgelegt.
  - Wert;Wert;Wert;...: Für das Attribut werden die angegebenen Mehrfachwerte festgelegt.
  - ' ' (leer): Das Attribut wird nicht geändert.
  - NULL: Das Attribut wird gelöscht. Für die Löschsequenz wird standardmäßig NULL festgelegt. Dieser Wert kann jedoch im Fenster "Hochladen von Dateien des Massendatenladers - Suche" bearbeitet werden.

Hinweis: Wenn Sie ein # in der Feeder-Datei verwenden möchten, setzen Sie das Zeichen in doppelte Anführungszeichen, z. B. sollten Sie user#1 als "user#1" angeben.

Wichtig! Die Feeder-Datei muss UTF-8-kodiert gespeichert werden.

Beispiel-Feeder-Datei für das Erstellen von Benutzern

Diese Beispiel-Feeder-Datei erstellt Benutzer mit gewissen erforderlichen Attributen.

```
action,%USER_ID%,%FIRST_NAME%,%LAST_NAME%,%FULL_NAME%,%PASSWORD%,%EMAIL%
create,JD,John,Doe,John Doe,mypassword,Johndoe@a.com
create,BD,Baby,Doe,Baby Doe,mypassword2,Babydoe@a.com
```

Im vorstehenden Code weist die Feeder-Datei die folgenden Eigenschaften auf:

Header

Bei der ersten Zeile des Code handelt es sich um die Header-Zeile. Die Header-Zeile enthält physische bzw. bekannte Attribute für das verwaltetet Objekt "Benutzer".

Aktion

In der Aktionsspalte ist die Aufgabe angegeben, die für jeden Datensatz ausgeführt werden soll. In der vorstehenden Datei ist beispielsweise angegeben, dass die Aktion "create" für den Vornamen (First Name) "John" ausgeführt werden soll.

Beispiel-Feeder-Datei für das Aktivieren von Benutzern

Diese Beispiel-Feeder-Datei ändert den Wert des logischen Attributs |enabled|. Sie geben das logische Attribut im Header und den Wert (in diesem Fall "true" oder "false") in jeder Benutzereingabe in der Datei an.

```
action,%USER_ID%,|enable|

MODIFY,user1,false

MODIFY,user2,true
```

Registerkarte "Details der Loader-Datensätze"

Die Registerkarte "Details der Loader-Datensätze" zeigt eine kurze Vorschau der Datensätze an, die in Ihrer Feeder-Datei verfügbar sind. Die Vorschautabelle zeigt maximal 5 Datensätze an. Anhand der Vorschautabelle können Benutzer überprüfen, ob sie die richtige Datei hochladen. Außerdem können Sie auf dieser Registerkarte die Art der Aktion angeben, die auf den in Ihrer Feeder-Datei genannten verwalteten Objekten durchgeführt werden soll. Sie müssen die folgenden Felder ausfüllen:

Welches Feld stellt die Aktion dar, die auf dem Objekt durchgeführt werden soll?

Gibt die Felder aus der Feeder-Datei an, die die auf den verwalteten Objekten durchzuführenden Aktionen beschreiben. Beispielsweise können Sie eine Feeder-Datei mit einem Feld "Aktion" verwenden, das die Werte "Erstellen", "Ändern" und "Löschen" annehmen kann. Sie müssen jede dieser Aktionen in Zuordnung der Loader-Aktionen (siehe Seite 570) einer Admin-Aufgabe zuordnen.

Welches Feld wird zur eindeutigen Identifizierung des Objekts verwendet?

Identifiziert das Feld aus der Feeder-Datei, mit der das primäre Objekt eindeutig identifiziert werden kann.

Hinweis: Wenn die Feeder-Datei eine ungültige Kopfzeile hat, werden die Datensätze der Feeder-Datei nicht auf der Registerkarte "Details der Loader-Datensätze" angezeigt. Wenn die Feeder-Datei eine ungültige Kopfzeile hat, wählen Sie eine andere Datei aus. Wenn die Feeder-Datei einige ungültige Datensätze enthält, wird der detaillierte Status des Hochladens unter der Registerkarte "System" auf der Registerkarte "Gesendete Aufgaben anzeigen" angezeigt.

Registerkarte "Zuordnung der Loader-Aktionen"

Die Registerkarte "Zuordnung der Loader-Aktionen" ermöglicht Ihnen die Auswahl eines primären Objekts, für das die in der Feeder-Datei festgelegten Aktionen durchgeführt werden. Sie müssen die Aktionen aus der Feeder-Datei auch zu Admin-Aufgaben für das ausgewählte primäre Objekt zuordnen.

Was ist das primäre Objekt?

Identifiziert das primäre Objekt, das von CA IdentityMinder mit Hilfe der Feeder-Datei manipuliert wird. Sie können eines der folgenden primären Objekte auswählen:

- User
- Gruppen
- Organisation

Wählen Sie eine Aufgabe zur Ausführung für "Aktion" aus.

Identifiziert die Admin-Aufgaben, die für jede in der Feeder-Datei festgelegte Aktion, z. B. die Aufgaben "Löschen" oder "Ändern", durchgeführt werden sollen.

Hinweis: Sie müssen alle Aktionen in der Feeder-Datei einer Admin-Aufgabe zuordnen. Außerdem hängen die in diesem Feld angezeigten Admin-Aufgaben von dem ausgewählten primären Objekt ab. Wenn Sie beispielsweise "Benutzer" als das primäre Objekt auswählen, werden nur die Admin-Aufgaben im Zusammenhang mit "Benutzer" angezeigt.

Wählen Sie für "Aktion" eine Aufgabe für ein noch nicht vorhandenes Objekt aus.

Sie identifiziert die alternativen Admin-Aufgaben, die für eine in der Feeder-Datei angegebene Aktion ausgeführt werden sollen, wenn das verwaltete Objekt noch nicht in CA IdentityMinder existiert, z. B. die Aufgabe "Erstellen".

Registerkarte "Laderbenachrichtigungs-Details"

Wichtig! Standardmäßig ist diese Registerkarte nicht in den Massendatenlader-Assistenten eingeschlossen. Sie müssen sie manuell hinzufügen, indem Sie die Massendatenlader-Aufgabe ändern und die Registerkarte "Laderbenachrichtigungs-Details" hinzufügen. Außerdem erfordert diese Registerkarte, dass Sie den Workflow in der Umgebung aktivieren.

Mithilfe der Registerkarte "Laderbenachrichtigungs-Details" können Sie Zertifizierungs-Manager für die Massendatenlader-Aufgabe auswählen. Wenn eine Massendatenlader-Aufgabe abgeschlossen ist, erstellt CA IdentityMinder eine Massendatenlader-Benachrichtigung für alle für die Aufgabe konfigurierten Zertifizierungs-Manager. Diese Benachrichtigung wird auf der Registerkarte "Startseite" unter den Massendatenladerbenachrichtigungen angezeigt. Beim Anklicken zeigt die Benachrichtigung Details für die vom Massenladungsvorgang initiierten Aufgaben an. Die Zertifizierungs-Manager können dann die in den Benachrichtigungen angegebenen Änderungen überprüfen und bestätigen.

Hinweis: Um eine Liste von Zertifizierungs-Managern anzugeben, verwenden Sie eine der verfügbaren Teilnehmerauflösungen in der Dropdown-Liste. Weitere Informationen über Teilnehmerauflösungen finden Sie im Workflow-Abschnitt dieses Handbuchs.

Bestätigen von Änderungen in der Massendatenlader-Aufgabe

Die Massendatenladerbenachrichtigungen enthalten Details zu allen Änderungen, die die Massendatenlader-Aufgabe initiiert hat. Zertifizierungs-Manager können von einer Massendatenlader-Aufgabe initiierte Änderungen überprüfen und bestätigen.

So überprüfen und bestätigen Sie Änderungen durch Massendatenlader-Aufgaben:

1. Melden Sie sich bei der Benutzerkonsole als ein Benutzer an, der als ein Zertifizierungs-Manager für eine Massendatenlader-Aufgabe aufgelistet wird.
2. Wechseln Sie zur Startseite, "Meine Massendatenladerbenachrichtigungen anzeigen".

3. Wählen Sie die Massendatenladerbenachrichtigung aus, die Sie überprüfen wollen.

   Das Massendatenladerbenachrichtigungs-Fenster wird geöffnet und zeigt eine Tabellenauflistung aller Massendatenlader-Aufgabenänderungen an, die initiiert wurden.

   In diesem Fenster können Sie Folgendes ausführen:

   - Um bestimmte Aufgabendetails für eine Objekterstellung oder -änderung zu überprüfen, klicken Sie auf den Hyperlink unter der Beschreibungsspalte.
   - Wenn es Compliance-Verletzungen gibt oder wenn Sie eine Rolle entfernen wollen, die einem Benutzer hinzugefügt wurde, können Sie den Benutzer direkt vom Benachrichtigungsfenster aus bearbeiten, indem Sie auf das Bearbeitungssymbol neben der Benutzer-ID klicken.
   - Um einem Benutzer hinzugefügte Rollen zu überprüfen, klicken Sie auf den Hyperlink unter der Spalte "Angeforderte Rollenzuweisungen" für die Benutzer-ID.

4. Sobald Sie alle Änderungen für ein bestimmtes Objekt überprüft haben, aktivieren Sie das Kontrollkästchen "Bestätigen" für dieses Objekt.

5. Sobald Sie alle Änderungen bestätigt haben, klicken Sie auf "Bestätigen", um alle ausgewählten Änderungsbenachrichtigungen aus der Liste zu entfernen.

   Hinweis: Sie können "Alle bestätigen" auswählen, um alle Änderungen in einer Massendatenladerbenachrichtigung zu bestätigen. Dies löscht die Massendatenladerbenachrichtigung aus der Registerkarte "Startseite". Außerdem können Sie das Kontrollkästchen oben in der Spalte "Bestätigen" aktivieren, um alle Änderungsbenachrichtigungen im Fenster zu diesem Zeitpunkt auszuwählen und die Änderungen Fenster für Fenster zu bestätigen.

   Wenn alle mit einer Massendatenlader-Aufgabe verbundenen Benutzeränderungen bestätigt werden, wird die Massendatenladerbenachrichtigung von der Registerkarte "Startseite" entfernt.

Konfigurieren von E-Mail-Benachrichtigungen für Massendatenlader-Aufgaben

In manchen Umgebungen sind E-Mail-Benachrichtigungen für Massenaufgaben standardmäßig konfiguriert. Um zu überprüfen, ob E-Mail-Benachrichtigungen für Massenaufgaben in Ihrem System konfiguriert sind, gehen Sie zu "System", "E-Mail", "E-Mail anzeigen", und suchen Sie nach dem Begriff "Masse".

Wenn keine E-Mail-Benachrichtigungen in Ihrer Umgebung konfiguriert sind, konfigurieren Sie die E-Mail, die gesendet wird, wenn ein Massenvorgang abschließt.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Benutzerkonsole auf "System", "E-Mail" und "E-Mail erstellen".
2. Füllen Sie die erforderlichen Felder in der Registerkarte "Profil" aus.
3. Führen Sie auf der Registerkarte "Sendezeitpunkt" die folgenden Schritte aus:
   a. Wählen Sie im ersten Feld "Aufgabe abgeschlossen" aus.
   b. Wählen Sie im zweiten Feld "Massendatenlader" aus.
4. Füllen Sie die Registerkarten "Empfänger" und "Inhalt" aus und klicken Sie auf "Senden".

   Die E-Mail-Benachrichtigungen wurden für Massendatenlader-Aufgaben konfiguriert.

Planen der Aufgabe "Massendatenlader"

Die Aufgabe "Massendatenlader" kann im System geplant werden. Dazu müssen Sie der Aufgabe die Registerkarte "Scheduler" hinzufügen (siehe Seite 70).

Ändern der Parser-Datei für den Massendatenlader

Wenn Sie den Parser ändern möchten, der für die Analyse von Feeder-Dateien verwendet wird, konfigurieren Sie die entsprechende Admin-Aufgabe.

So ändern Sie die Admin-Aufgabe "Massendatenlader"

1. Klicken Sie auf "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe ändern".
2. Suchen Sie die Aufgabe "Massendatenlader".
3. Wählen Sie die Aufgabe "Massendatenlader" aus und klicken Sie auf "Auswählen".
4. Wählen Sie die Registerkarte "Suchen" für die Aufgabe "Massendatenlader" aus.

5. Klicken Sie auf "Durchsuchen", um nach Suchfenstern zu suchen.

   Die Liste der verfügbaren Suchfenster wird angezeigt.

6. Wählen Sie ein Suchfenster aus und klicken Sie auf "Bearbeiten".

   Die Details des Suchfensters werden angezeigt.

7. (Optional) Bearbeiten Sie den voll qualifizierten Namen des Parsers.

   Der voll qualifizierte Name des Parsers muss mit dem Namen Ihrer Parser-Datei übereinstimmen.

   Hinweis: Weitere Informationen zum Erstellen eines benutzerdefinierten CSV-Parser finden Sie in der Javadoc für die FeederParser-Klasse. Wenn Sie JBoss als Ihren Anwendungsserver benutzen und Sie einen benutzerdefinierten Parser erstellen, muss sich die benutzerdefinierte Parserdatei im Verzeichnis iam_im.ear/user_console_war/WEB-INF/classes befinden.

8. Klicken Sie auf "OK".

Webservice-Unterstützung für den Massendatenlader

Der Massendatenlader besitzt eine Webdienst-API, die über die Task Execution Web Service (TEWS)-Schnittstelle von CA IdentityMinder aufgerufen werden kann. Über TEWS können Client-Anwendungen Remote-Aufgaben zur Ausführung an CA IdentityMinder senden. Diese Schnittstelle implementiert die offenen Standards WSDL und SOAP, um einen Remote-Zugriff auf CA IdentityMinder zu ermöglichen.

CA IdentityMinder enthält Beispiele für Java-Clients, die den Aufruf des Massendatenladers als Webdienst veranschaulichen. Die Java-Beispiele befinden sich in folgender Quelldatei:

admin_tools\samples\WebService\Axis\optional\ObjectsFeeder.java

Musterdaten sowie die Dokumentation für den Aufruf des Massendatenladers als Webservice befinden sich in folgendem Verzeichnis:

admin_tools\samples\Feeder\

Hinweis: Weitere Informationen finden Sie im *Programmierhandbuch für Java*.

JDBC-Verbindungsverwaltung

Informationen für CA IdentityMinder-Berichte können aus unterschiedlichen Quellen stammen. Jeder Bericht muss einer spezifischen Datenquelle zugeordnet werden, je nachdem, welche Informationen der Bericht enthalten soll.

Sollen für die Berichterstellung verschiedene Datenquellen eingerichtet werden (z. B. eine Audit- oder Aufgaben-Persistenz-Datenbank), müssen Sie in CA IdentityMinder ein verwaltetes Verbindungsobjekt erstellen. Nach dem Erstellen der Verbindung können Sie einem Bericht ein spezifisches verwaltetes Verbindungsobjekt zuweisen, indem Sie die Berichtsaufgabe ändern und unterhalb des Registers "Suchen" der Berichtsaufgabe die Einstellung "Verbindungsobjekt für den Bericht" festlegen.

JDBC-Verbindung erstellen

Gehen Sie folgendermaßen vor, wenn Sie in CA IdentityMinder Verbindungsdetails angeben möchten:

So erstellen Sie eine JDBC-Verbindung:

1. Klicken Sie auf "System", "JDBC-Verbindungsverwaltung", "JDBC-Verbindung herstellen".
2. Erstellen Sie ein neues Verbindungsobjekt, oder wählen Sie ein Verbindungsobjekt basierend auf einer spezifischen JNDI-Datenquelle aus.
3. Füllen Sie alle erforderlichen Felder aus, und klicken Sie auf "Senden".

   Es wird eine neue JDBC-Verbindung erstellt.

Logical-Attribute-Handler

Logische CA IdentityMinder-Attribute ermöglichen die Anzeige von Benutzerspeicherattributen (physische Attribute) in einem von Benutzern lesbaren Format in Aufgabenfenstern. CA IdentityMinder-Administratoren verwenden Aufgabenfenster, um Funktionen in CA IdentityMinder auszuführen. Logische Attribute sind in Benutzerspeichern nicht vorhanden. In der Regel stellen sie mindestens ein physisches Attribut dar, um die Darstellung zu vereinfachen. Das logische Attribut "Datum" kann beispielsweise die physischen Attribute "Tag", "Monat" und "Jahr" darstellen.

Logische Attribute werden von Logical-Attribute-Handlern verarbeitet, bei denen es sich um Java-Objekte handelt, die mit der Logical-Attribute-API geschrieben werden. (Weitere Hinweise finden Sie im *Programmierhandbuch für Java*.) Wenn beispielsweise ein Aufgabenfenster angezeigt wird, wandelt ein Logical-Attribute-Handler physische Attributdaten aus einem Benutzerspeicher in logische Attributdaten um, die im Aufgabenfenster angezeigt werden. Sie können die vordefinierten logischen Attribute und Logical-Attribute-Handler verwenden, die in CA IdentityMinder enthalten sind oder mit der Logical-Attribute-API neue erstellen.

Hinweis: Weitere Informationen zu logischen Attributen finden Sie im *Programmierhandbuch für Java*.

In der -Benutzerkonsole enthält die Unternehmenskategorie Aufgaben für die Verwaltung von Logical-Attribute-Handlern. Die Liste umfasst vordefinierte Handler, die in CA IdentityMinder enthalten sind, sowie alle an Ihrem Standort definierte, angepasste Handler.

Über die Unternehmensaufgabenkategorie haben Sie folgende Möglichkeiten:

- Erstellen neuer Logical-Attribute-Handler mit CA IdentityMinder
- Kopieren von Handlern
- Löschen von Handlern
- Ändern vorhandener Handler-Konfigurationen

Hinweis: Verwenden Sie zum Ändern der Ausführungsreihenfolge von Logical-Attribute-Handlern die Management-Konsole.

Erstellen von Logical-Attribute-Handlern

So erstellen Sie Logical-Attribute-Handler:

1. Wählen Sie "System", "Logical-Attribute-Handler erstellen".
2. Wählen Sie im Fenster "Logical-Attribute-Handler erstellen" die Option "Standardmäßigen Logical-Attribute-Handler erstellen" aus, und klicken Sie auf "OK".

3. Konfigurieren Sie im Fenster "Logical-Attribute-Handler erstellen" die Einstellungen für den Logical-Attribute-Handler.

   Klicken Sie in diesem Fenster auf den Hilfe-Link, um eine Beschreibung zu jedem Feld anzuzeigen.

4. Klicken Sie auf "Senden".

   Der Handler wird zur Liste der Handler im Fenster "Logical-Attribute-Handler" hinzugefügt.

Hinweis: Nach dem Konfigurieren von Logical-Attribute-Handlern mit der Benutzerkonsole muss der Anwendungsserver nicht neu gestartet werden.

Kopieren von Logical-Attribute-Handlern

So kopieren Sie Logical-Attribute-Handler:

1. Wählen Sie "System", "Logical-Attribute-Handler erstellen".
2. Wählen Sie im Fenster "Logical-Attribute-Handler erstellen" die Option "Kopie einer Logical-Attribute-Handler-Definition erstellen" aus, und klicken Sie auf "Suchen".
3. Wählen Sie einen Logical-Attribute-Handler aus (z. B. "ConfirmPasswordHandler"), und klicken Sie auf "OK".
4. Konfigurieren Sie im Fenster "Logical-Attribute-Handler erstellen" die Einstellungen für den Logical-Attribute-Handler.

   Klicken Sie in diesem Fenster auf den Hilfe-Link, um eine Beschreibung zu jedem Feld anzuzeigen.

5. Klicken Sie auf "Submit".

   Der Handler wird zur Liste der Handler im Fenster "Logical-Attribute-Handler" hinzugefügt.

Hinweis: Nach dem Konfigurieren von Logical-Attribute-Handlern mit der Benutzerkonsole muss der Anwendungsserver nicht neu gestartet werden.

Erstellen des Logical-Attribute-Handler "ForgottenPasswordHandler"

Der Logical-Attribute-Handler "ForgottenPasswordHandler" verwendet für folgende Funktionen unterschiedliche logische Attribute:

- Konfiguration
- Laufzeitfragen und -antworten

So erstellen Sie den Logical-Attribute-Handler "ForgottenPasswordHandler":

1. Wählen Sie "System", "Logical-Attribute-Handler erstellen".
2. Wählen Sie im Fenster "Logical-Attribute-Handler erstellen" die Option "Standardmäßigen Logical-Attribute-Handler erstellen" aus, und klicken Sie auf "Suchen".
3. Wählen Sie "ForgottenPasswordHandler" aus, und klicken Sie auf OK.
4. Konfigurieren Sie im Fenster "Logical-Attribute-Handler erstellen: ForgottenPasswordHandler" die Einstellungen für den Logical-Attribute-Handler.

   Klicken Sie in diesem Fenster auf den Hilfe-Link, um eine Beschreibung zu jedem Feld anzuzeigen.
5. Klicken Sie auf "Senden".

   Der Handler wird zur Liste der Handler im Fenster "Logical-Attribute-Handler" hinzugefügt.

Hinweis: Nach dem Konfigurieren von Logical-Attribute-Handlern mit der Benutzerkonsole muss der Anwendungsserver nicht neu gestartet werden.

Löschen von Logical-Attribute-Handlern

So löschen Sie Logical-Attribute-Handler:

1. Wählen Sie "System > Logical-Attribute-Handler löschen".
2. Aktivieren Sie im Fenster "Logical-Attribute-Handler löschen" das Kontrollkästchen links von allen logischen Attributen, die gelöscht werden sollen.
3. Klicken Sie auf "Auswählen".

   In CA IdentityMinder wird eine Bestätigungsmeldung angezeigt.
4. Klicken Sie auf "Ja", um den Löschvorgang zu bestätigen.

Ändern von Logical-Attribute-Handlern

So ändern Sie Logical-Attribute-Handler:

1. Wählen Sie "System > Logical-Attribute-Handler ändern"**.**
2. Wählen Sie im Fenster "Logical-Attribute-Handler ändern" den Handler aus, den Sie ändern möchten, und klicken Sie auf "Auswählen".
3. Wählen Sie einen Logical-Attribute-Handler aus (z. B. "ConfirmPasswordHandler"), und klicken Sie auf "OK".

4. Konfigurieren Sie im Fenster "Logical-Attribute-Handler ändern" die Einstellungen für den Logical-Attribute-Handler.

   Klicken Sie in diesem Fenster auf den Hilfe-Link, um eine Beschreibung zu jedem Feld anzuzeigen.

5. Klicken Sie auf "Senden".

Hinweis: Nach dem Konfigurieren von Logical-Attribute-Handlern mit der Benutzerkonsole muss der Anwendungsserver nicht neu gestartet werden.

Anzeigen von Logical-Attribute-Handlern

So zeigen Sie Logical-Attribute-Handler an:

1. Wählen Sie "System > Logical-Attribute-Handler anzeigen".
2. Wählen Sie im Fenster "Logical-Attribute-Handler anzeigen" den Handler aus, den Sie anzeigen möchten, und klicken Sie auf "Auswählen".
3. Sehen Sie die Eigenschaften des Logical-Attribute-Handler ein, und klicken Sie auf "Schließen".

Auswahlfelddaten

Sie können die in folgenden Feldern verfügbaren Optionen auffüllen:

- Mehrfachauswahl-Kontrollkästchen
- Dropdown
- Dropdown-Kombinationsfeld
- Mehrfachauswahl
- Optionsauswahl
- Kombinationsfeld für Optionsauswahl

- Optionsfeld mit Einfach-Auswahl
- Einfachauswahl

Diese Optionen werden in den XML-Dateien für die Felddatenauswahl gespeichert. Sie können beispielsweise die XML-Dateien "Auswahlfelddaten" verwenden, um Optionen für das Dropdown-Feld "Stadt" oder "Bundesstaat" auf der Registerkarte "Profil" für die Aufgabe "Benutzer erstellen" zu füllen.

Mit Hilfe der XML-Dateien für die Felddatenauswahl können Sie auch eine Abhängigkeit zwischen zwei Feldern in einer Admin-Aufgabe konfigurieren. Die Optionen im Feld "Stadt" können beispielsweise von der Option abhängen, die ein Benutzer für das Feld "Bundesstaat" auswählt.

Hinweis: Weitere Informationen zu Auswahlfelddaten finden Sie im *User Console Design Guide.*

Aufgabenfenster "Korrelationsattribute konfigurieren"

Dieses Thema ist nur für CA CloudMinder relevant.

Verwenden Sie das Aufgabenfenster "Korrelationsattribute konfigurieren", um Korrelationsregeln für die Umgebung zu konfigurieren.

CA IdentityMinder liest Konfigurationsparameter in den Arbeitsspeicher und synchronisiert regelmäßig die Arbeitsspeicherversion mit der Datenbankversion des gängigen DSA. Da die Korrelationsattribute mandantenspezifisch sind, liest der Bereitstellungsserver die Korrelationsattribute vom entsprechenden Mandanten-DSA während eines Durchsuchungs- und Korrelationsvorgangs. Die aktualisierten Korrelationsregeln treten sofort in Kraft, ohne die Parameteraktualisierung abwarten zu müssen.

Aufgabenfenster "Auf globaler Richtlinie basierter Workflow für Ereignisse konfigurieren"

Die Aufgabe "Auf globaler Richtlinie basierter Workflow für Ereignisse konfigurieren" ermöglicht einem Administrator die Konfiguration eines richtlinienbasierten oder nicht richtlinienbasierten Workflows für alle Ereignisse in der aktuellen Umgebung. Wenn die Aufgabe angeklickt wird, wird die standardmäßige Ereigniszuordnung zu Workflow-Prozessdefinitionen angezeigt. Jede Ereigniszuordnung kann geändert oder gelöscht werden, und es können neue Ereigniszuordnungen für Ereignisse hinzugefügt werden, die noch nicht konfiguriert wurden.

Dieses Fenster enthält die folgenden Felder:

Workflow-Prozesse, die Ereignissen in dieser Umgebung zugeordnet sind.

Gibt die mit Genehmigungsrichtlinien verknüpften Workflow-Prozesse an.

Neue Zuordnungen hinzufügen

Gibt eine Genehmigungsrichtlinie an, die einem Workflow-Prozess zugeordnet werden soll.

Schaltfläche "Hinzufügen"

Fügt die neue Zuordnung hinzu.

Wenn Sie eine Zuordnung hinzufügen oder ändern, wird das Fenster für die Workflow-Zuordnung angezeigt, in dem Sie die Prozesszuordnungen und Genehmigungsrichtlinien auswählen können. Das Verhalten ist dasselbe wie bei der Workflow-Konfiguration auf Ereignisebene. Wenn Sie auf der Seite für die Workflow-Zuordnungen auf die Schaltfläche "Hinzufügen" klicken, wird eine andere Seite angezeigt, auf der Sie eine Genehmigungsrichtlinie konfigurieren können.

Weitere Informationen:

Konfigurieren des richtlinienbasierten Workflows für Ereignisse (siehe Seite 353)
Konfigurieren einer Genehmigungsrichtlinie (siehe Seite 356)

Aufgabenstatus in CA IdentityMinder

Unter Umständen möchten Administratoren den Status von CA IdentityMinder-Aufgaben verfolgen, nachdem sie zur Verarbeitung übermittelt wurden. In CA IdentityMinder stehen die folgenden Methoden zum Anzeigen des Aufgabenstatus zur Verfügung:

- **Registerkarte "Übermittelte Aufgaben anzeigen"**

  Mit dieser Registerkarte können Sie nach CA IdentityMinder-Aufgaben suchen und diese anzeigen, die zur Verarbeitung übermittelt wurden.

  Administratoren können eine Zusammenfassung der Aufgabendetails oder zusätzliche Details anzeigen.

  Registerkarte "Übermittelte Aufgaben anzeigen" ist in zwei Standardaufgaben enthalten:

  - Meine gesendeten Aufgaben anzeigen

    Ermöglicht es Administratoren, nach Informationen von Aufgaben zu suchen und diese anzuzeigen, die sie zur Verarbeitung übermittelt haben.

  - Gesendete Aufgaben anzeigen

    Ermöglicht es Administratoren, nach Informationen von Aufgaben zu suchen und diese anzuzeigen, die andere Administratoren zur Verarbeitung übermittelt haben.

- **Registerkarte "Benutzerverlauf"**

  Mit dieser Registerkarte, die zu Benutzeraufgaben wie "Ansicht" oder "Benutzer ändern" hinzugefügt werden kann, können Administratoren die folgenden Informationen für die ausgewählten Benutzer anzeigen:

  - Aufgaben, die für den Benutzer durchgeführt wurden
  - Aufgaben, die vom Benutzer durchgeführt wurden
  - Workflow-Genehmigung dieses Benutzers

- **Berichte**

  CA IdentityMinder-Berichte ermöglichen die Anzeige des aktuellen Status einer CA IdentityMinder-Umgebung. Anhand dieser Informationen können Sie die Konformität mit internen Geschäftsrichtlinien oder externen Vorschriften gewährleisten.

  Im Abschnitt zu Berichten finden Sie weitere Informationen zum Einrichten und Verwenden von Berichten.

- **Protokolle**

  Sie zeigen Informationen zu allen Komponenten in einer CA IdentityMinder-Installation an und machen Details zu allen Vorgängen in CA IdentityMinder verfügbar.

  Im *Konfigurationshandbuch* finden Sie weitere Informationen zu CA IdentityMinder-Protokollen.

So legt CA IdentityMinder den Aufgabenstatus fest

Bei einer *Aufgabe* handelt es sich um eine Verwaltungsfunktion, die Benutzer in CA IdentityMinder ausführen können. Aufgaben beinhalten *Ereignisse*. Hierbei handelt es sich um Aktionen, die von CA IdentityMinder zum Abschließen von Aufgaben ausgeführt werden. Eine Aufgabe kann mehrere Ereignisse umfassen. So kann beispielsweise die Aufgabe "Benutzer erstellen" Ereignisse für das Erstellen des Benutzerprofils, das Hinzufügen des Benutzers zu einer Gruppe und das Zuweisen von Rollen beinhalten.

CA IdentityMinder-Aufgaben und -Ereignisse können mit Workflow-Prozessen verknüpft werden, die bestimmen, wie in CA IdentityMinder die erforderlichen Aktionen und andere benutzerdefinierte Geschäftslogik ausgeführt werden. Aufgaben können auch mit anderen Aufgaben verknüpft werden, die als verschachtelte Aufgaben bezeichnet werden. In diesem Fall werden die verschachtelten Aufgaben von CA IdentityMinder zusammen mit der ursprünglichen Aufgabe ausgeführt.

Der Status einer Aufgabe hängt vom Status der mit ihr verknüpften Ereignisse, Workflow-Prozesse, verschachtelten Aufgaben und benutzerdefinierten Geschäftslogiken ab.

Gesendete Aufgaben anzeigen

In CA IdentityMinder ist die Funktion "Gesendete Aufgaben anzeigen" enthalten, die Informationen zu Aufgaben in einer CA IdentityMinder-Umgebung enthält. Sie können diese Funktion verwenden, um nach hochwertigen Details zu Aktionen, die in CA IdentityMinder ausgeführt werden, zu suchen und diese anzuzeigen. Detailfenster bieten zusätzliche Informationen zu jeder Aufgabe und jedem Ereignis.

Sie können eine Aufgabe abhängig von ihrem Status mit Hilfe der Funktion "Gesendete Aufgaben anzeigen" abbrechen oder erneut senden.

Mit der Funktion "Gesendete Aufgaben anzeigen" können Sie die Verarbeitung einer Aufgabe von Anfang bis Ende verfolgen. Wenn eine CA IdentityMinder-Aufgabe beispielsweise die Zuweisung von Bereitstellungsrollen umfasst und diese Zuweisung die Erstellung von Konten in anderen Systemen auslöst, zeigt die Registerkarte "Gesendete Aufgaben anzeigen" alle Details der ursprünglichen Aufgabe und die Details der Kontenerstellungen an.

Die Registerkarte "Gesendete Aufgaben anzeigen" enthält Details zu den im System ausgeführten Vorgängen. Diese Vorgänge können das Ergebnis eines CA IdentityMinder-Ereignisses wie "EnableUserEvent" sein. Die vom System gesendeten Benachrichtigungen sind unterhalb dieses Ereignisses gruppiert. Die Registerkarte "Gesendete Aufgaben anzeigen" zeigt eine Meldung an, die darauf hinweist, dass sich die Benachrichtigungen in Bearbeitung befinden, bis die Benachrichtigung "End Detail" gesendet wird. Anschließend wechselt die Meldung in "Abgeschlossen".

Standardmäßig ist die Registerkarte "Gesendete Aufgaben anzeigen" in CA IdentityMinder in zwei Aufgaben enthalten:

- Gesendete Aufgaben anzeigen
- Meine gesendeten Aufgaben anzeigen

Suchen nach gesendeten Aufgaben

Führen Sie die folgenden Schritte aus, um nach gesendeten Aufgaben zu suchen.

So suchen Sie nach gesendeten Aufgaben:

1. Klicken Sie auf "System", "Gesendete Aufgaben anzeigen".

   Die Seite "Gesendete Aufgaben anzeigen" wird angezeigt.

2. Geben Sie Suchkriterien und die Anzahl der anzuzeigenden Zeilen an, und klicken Sie auf "Suchen".

   Die Aufgaben, die Ihre Suchkriterien erfüllen, werden angezeigt.

   Hinweis: Weitere Informationen dazu, wie Sie Attribute in den Suchkriterien angeben, finden Sie in Suchattribute zum Anzeigen von gesendeten Aufgaben (siehe Seite 585).

Suchattribute zum Anzeigen von gesendeten Aufgaben

Um Aufgaben zu überprüfen, die zur Verarbeitung gesendet wurden, können Sie die Suchfunktion in "Gesendete Aufgaben anzeigen" verwenden. Sie können basierend auf folgenden Kriterien nach Aufgaben suchen:

Initiiert von

Gibt den Namen des Benutzers, der die Aufgabe initiiert hat, als Suchkriterium an. Suchen basieren auf dem Benutzernamen. Um sicherzustellen, dass Sie einen gültigen Benutzernamen eingegeben haben, klicken Sie auf die Schaltfläche "Validieren".

Genehmigungsaufgaben durchgeführt von

Gibt den Namen des Aufgabengenehmigers als Suchkriterium an. Suchen basieren auf dem Benutzernamen. Um sicherzustellen, dass Sie einen gültigen Benutzernamen eingegeben haben, klicken Sie auf die Schaltfläche "Validieren".

Hinweis: Wenn Sie das Kriterium "Genehmigungsaufgaben durchgeführt von" auswählen, um die Aufgaben zu filtern, ist das Kriterium "Genehmigungsaufgaben anzeigen" standardmäßig ebenfalls aktiviert.

Aufgabenname

Gibt den Aufgabennamen als Suchkriterium an. Sie können die Suche mit dem Wert des Feldes "Mit Aufgabennamen" verfeinern, indem Sie Bedingungen wie "gleich", "enthält", "startet mit" oder "endet auf" angeben. Sie können beispielsweise das Suchkriterium "Aufgabenname gleich Benutzer erstellen" angeben, indem Sie die Bedingung "gleich" auswählen und im Textfeld "Benutzer erstellen" eingeben.

Aufgabenstatus

Gibt den Aufgabenstatus als Suchkriterium an. Sie können den Aufgabenstatus auswählen, indem Sie "mit Aufgabenstatus gleich" aktivieren und die Bedingung auswählen. Basierend auf den folgenden Bedingungen können Sie die Suche noch weiter verfeinern:

- Abgeschlossen
- In Bearbeitung
- Fehlgeschlagen
- Abgelehnt
- Teilweise abgeschlossen
- Abgebrochen
- Geplant

Hinweis: Weitere Informationen finden Sie unter Beschreibungen des Aufgabenstatus (siehe Seite 587).

Aufgabenpriorität

Gibt die Aufgabenpriorität als Suchkriterium an. Sie können die Aufgabenpriorität auswählen, indem Sie "mit Aufgabenpriorität gleich" aktivieren und die Bedingung auswählen. Basierend auf den folgenden Bedingungen können Sie die Suche noch weiter verfeinern:

Niedrig

Gibt an, dass Sie nach Aufgaben mit der Priorität "Niedrig" suchen können.

Mittel

Gibt an, dass Sie nach Aufgaben mit der Priorität "Mittel" suchen können.

Hoch

Gibt an, dass Sie nach Aufgaben mit der Priorität "Hoch" suchen können.

Ausgeführt für

Gibt Aufgaben an, die für die ausgewählte Instanz des Objekts ausgeführt werden. Wenn Sie keine Instanz des Objekts auswählen, werden die Aufgaben angezeigt, die für alle Instanzen dieses Objekts ausgeführt wurden.

Hinweis: Dieses Feld wird nur angezeigt, wenn das Feld "'Ausgeführt für' konfigurieren" im Fenster "Gesendete Aufgaben konfigurieren" ausgefüllt ist. Dieses Fenster wird zum Konfigurieren der Registerkarte "Gesendete Aufgaben" verwendet. In der Online-Hilfe zu diesem Fenster finden Sie weitere Informationen.

Datumsbereich

Gibt die Daten an, innerhalb derer Sie nach gesendeten Aufgaben suchen möchten. Sie müssen das Start- und Enddatum angeben.

Nicht gesendete Aufgaben anzeigen

Gibt Aufgaben mit dem Status "Überprüft" an. Gibt Aufgaben an, die andere Aufgaben initiiert haben oder die nicht gesendet wurden. Alle diese Aufgaben werden bei Auswahl dieser Registerkarte überprüft und angezeigt.

Genehmigungsaufgaben anzeigen

Gibt die Aufgaben an, die als Teil eines Workflow genehmigt werden müssen.

Archiv der gesendeten Aufgaben durchsuchen

Identifizieren Sie die gesendeten Aufgaben, die archiviert wurden.

Weitere Informationen:

Beschreibungen des Aufgabenstatus (siehe Seite 587)

Beschreibungen des Aufgabenstatus

Gesendete Aufgaben liegen in einem der unten beschriebenen Status vor. Je nach Status der Aufgabe können Sie Aktionen ausführen, wie Aufgaben abbrechen oder erneut senden.

Hinweis: Zum Abrechen oder erneuten Senden einer Aufgabe müssen Sie die Registerkarte "Gesendete Aufgaben anzeigen" so konfigurieren, dass die Schaltflächen zum Abbrechen und erneuten Senden basierend auf dem Status der Aufgaben angezeigt werden. Weitere Informationen zum Abbrechen und erneuten Senden von Aufgaben finden Sie unter Anpassen der Registerkarte "Gesendete Aufgaben anzeigen" (siehe Seite 590).

In Bearbeitung

Wird angezeigt, wenn einer der folgenden Zustände eintritt:

- Workflow wurde initiiert, aber noch nicht abgeschlossen
- Aufgaben, die vor den aktuellen Aufgaben initiiert werden, befinden sich in Bearbeitung
- Verschachtelte Aufgaben wurden initiiert, aber noch nicht abgeschlossen
- Das primäre Ereignis wurde initiiert, aber noch nicht abgeschlossen
- Sekundäre Ereignisse wurden initiiert, aber noch nicht abgeschlossen

Aufgaben mit diesem Status können abgebrochen werden.

Hinweis: Durch Abbrechen einer Aufgabe werden alle unvollständigen verschachtelten Aufgaben und Ereignisse der aktuellen Aufgabe abgebrochen.

Abgebrochen

Wird angezeigt, wenn Sie eine der Aufgaben oder eines der Ereignisse abbrechen, die in Bearbeitung sind.

Abgelehnt

Wird angezeigt, wenn CA IdentityMinder ein Ereignis oder eine Aufgabe ablehnt, die Teil eines Workflow-Prozesses ist. Abgelehnte Aufgaben können erneut gesendet werden.

Hinweis: Beim erneuten Senden von Aufgaben sendet CA IdentityMinder alle fehlgeschlagenen bzw. abgelehnten verschachtelten Aufgaben und Ereignisse erneut.

Teilweise abgeschlossen

Wird angezeigt, wenn einige der Ereignisse oder verschachtelten Aufgaben abgebrochen werden. Teilweise abgeschlossene Ereignisse und verschachtelte Aufgaben können erneut gesendet werden.

Abgeschlossen

Wird angezeigt, wenn eine Aufgabe abgeschlossen ist. Eine Aufgabe ist abgeschlossen, wenn die verschachtelten Aufgaben und Ereignisse der aktuellen Aufgabe abgeschlossen sind.

Fehlgeschlagen

Wird angezeigt, wenn eine Aufgabe, eine verschachtelte Aufgabe oder ein verschachteltes Ereignis in der aktuellen Aufgabe ungültig sind. Dieser Status wird angezeigt, wenn die Aufgabe fehlschlägt. Fehlgeschlagene Aufgaben können erneut gesendet werden.

Geplant

Wird angezeigt, wenn die Aufgabe so geplant ist, dass sie zu einem späteren Zeitpunkt ausgeführt wird. Aufgaben mit diesem Status können abgebrochen werden.

Überprüft

Wird angezeigt, wenn die aktuelle Aufgabe überprüft wurde.

Anzeigen von Aufgabendetails

In CA IdentityMinder stehen Aufgabendetails zur Verfügung, wie der Status von übermittelten Aufgaben, verschachtelte Aufgaben und Ereignisse, die Aufgaben zugeordnet sind.

So zeigen Sie Details einer übermittelten Aufgabe an:

1. Klicken auf der Registerkarte "Gesendete Aufgaben anzeigen" auf das Symbol mit dem Rechtspfeil neben der ausgewählten Aufgabe.

   Die Aufgabendetails werden angezeigt.

   Hinweis: Falls Ereignisse und verschachtelte Aufgaben vorhanden sind, werden diese auf der Seite "Aufgabendetails" angezeigt. Sie können die Aufgabendetails für alle Aufgaben und Ereignisse anzeigen.

2. Klicken Sie auf "Close".

   Die Registerkarte "Aufgabendetails" wird geschlossen und CA IdentityMinder zeigt die Registerkarte "Übermittelte Aufgaben anzeigen" mit der Aufgabenliste an.

Anzeigen von Ereignisdetails

In CA IdentityMinder stehen Ereignisdetails zur Verfügung, wie der Status von übermittelten Ereignissen, Ereignisattribute und alle weiteren zusätzlichen Informationen zu Ereignissen.

So zeigen Sie Details eines übermittelten Ereignisses an:

1. Klicken Sie auf der Seite "Aufgabendetails anzeigen" auf das Symbol mit dem Rechtspfeil neben einem Ereignis.

   Die Ereignisdetails werden angezeigt.

2. Klicken Sie auf "Close".

   Die Seite "Ereignisdetails" wird geschlossen.

Beschreibung des Ereignisstatus

Ereignisse in CA IdentityMinder können in den unten beschriebenen Status vorliegen. Je nach Ereignisstatus können Sie Ereignisse abbrechen oder erneut für die Ausführung senden.

Hinweis: Damit Administratoren Ereignisse abbrechen bzw. erneut senden können, müssen Sie die Registerkarte "Übermittelte Aufgaben anzeigen" so konfigurieren, dass die Schaltflächen "Abbrechen" und "Ereignisse erneut senden" angezeigt werden. Beim Konfigurieren von Aufgaben können Sie angeben, welche Administratoren Ereignisse abbrechen und erneut senden können. Weitere Informationen zum Abbrechen und erneuten Senden von Ereignissen finden Sie unter Anpassen der Registerkarte "Übermittelte Aufgaben anzeigen" (siehe Seite 590).

In Bearbeitung

Wird angezeigt, wenn einer der folgenden Zustände eintritt:

- Workflows oder vor Ereignissen stattfindende Aufgaben werden initiiert, sind in Bearbeitung oder werden genehmigt
- CA IdentityMinder führt das Ereignis aus
- CA IdentityMinder führt nach Ereignissen stattfindende Aufgaben aus

Ereignisse mit diesem Status können abgebrochen werden.

Abgelehnt

Wird angezeigt, wenn in CA IdentityMinder Ereignisse abgelehnt werden, die Teil des Workflow sind. Abgelehnte Ereignisse können erneut gesendet werden.

Abgebrochen

Wird angezeigt, wenn Sie eines der Ereignisse abbrechen, das in Bearbeitung ist. Abgebrochene Ereignisse können erneut gesendet werden.

Abgeschlossen

Wird angezeigt, wenn ein Ereignis abgeschlossen ist.

Fehlgeschlagen

Wird angezeigt, wenn in CA IdentityMinder während des Ausführens von Ereignissen eine Ausnahme auftritt. Abgebrochene Ereignisse können erneut gesendet werden.

Hinweis: Sekundäre Ereignisse können erst erneut gesendet werden, wenn das entsprechende primäre Ereignis abgeschlossen ist.

Geplant

Wird angezeigt, wenn das Ereignis so geplant ist, dass es zu einem späteren Zeitpunkt ausgeführt wird. Ereignisse mit diesem Status können abgebrochen werden.

Überprüft

Wird angezeigt, wenn das aktuelle Ereignis überprüft wurde.

Anpassen der Registerkarte "Gesendete Aufgaben anzeigen"

Sie können die Registerkarte "Gesendete Aufgaben anzeigen" wie folgt anpassen:

- Angeben eines anderen Aufgabennamens und -tags.
- Ändern der standardmäßigen Anzeigeeigenschaften. Bei der Standardinstallation wird den Benutzern ein Suchfenster angezeigt, auf dem sie Kriterien eingeben können, die die Aufgaben festlegen, die auf der Registerkarte angezeigt werden. Sie können die Registerkarte so konfigurieren, dass automatisch die gesendeten Aufgaben des aktuellen Tages angezeigt werden, so dass die Benutzer keine Suchkriterien mehr eingeben müssen.
- Festlegen, ob Überwachungsereignisse auf der Seite "Aufgabendetails" angezeigt werden.
- Hinzufügen einer zusätzlichen Spalte zur Aufgabenanzeige.
- Angeben der Kriterien zum Abbrechen oder erneuten Senden von Aufgaben und Ereignissen.

Hinweis: Einige Aufgaben- und Ereignisdetails können Daten wie Gehälter oder Kennwörter enthalten, die in der Registerkarte "Gesendete Aufgaben anzeigen" nicht im Klartext erscheinen sollten. Sie können diese Attribute verbergen, indem Sie bei der Definition der Attribute in der Datei "directory.xml" Datenklassifizierungsparameter angeben. Weitere Informationen zu der Datei "directory.xml" finden Sie im *Konfigurationshandbuch*.

Sie können die Registerkarte "Gesendete Aufgaben anzeigen" konfigurieren, indem Sie die entsprechende Admin-Aufgabe ändern.

So konfigurieren Sie die Registerkarte "Gesendete Aufgaben anzeigen":

1. Wählen Sie die Optionen "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe ändern" aus.

   Daraufhin wird die Seite "Admin-Aufgabe auswählen" angezeigt.

2. Wählen Sie im Feld "Admin-Aufgaben durchsuchen" die Option "Name" oder "Kategorie" aus, geben Sie die zu suchende Zeichenfolge ein, und klicken Sie dann auf "Suchen".

   Daraufhin werden in CA IdentityMinder die Admin-Aufgaben angezeigt, die den Suchkriterien entsprechen.

3. Wählen Sie "Gesendete Aufgaben anzeigen" aus, und klicken Sie auf "Auswählen".

   In CA IdentityMinder werden die Aufgabendetails für die Admin-Aufgabe "Gesendete Aufgaben anzeigen" angezeigt.

4. Klicken Sie auf die Registerkarte "Registerkarten".

   Die Registerkarten, die auf der Registerkarte "Gesendete Aufgaben anzeigen" verwendet werden, werden angezeigt.

5. Klicken Sie auf das Symbol mit dem Rechtspfeil, um die Registerkarte "Gesendete Aufgaben" zu bearbeiten.

   Die Registerkartendetails werden angezeigt.

6. Bearbeiten Sie die Felder, um die Registerkarte "Gesendete Aufgaben anzeigen" wie erforderlich anzupassen. Weitere Informationen finden Sie unter Konfigurationseinstellungen für die Registerkarte "Gesendete Aufgaben anzeigen" (siehe Seite 592).

Konfigurationseinstellungen für die Registerkarte "Übermittelte Aufgaben anzeigen"

Verwenden Sie die folgenden Felder, um die Darstellung und die Funktionen der Registerkarte "Übermittelte Aufgaben anzeigen" zu ändern.

Name

Gibt den Namen der Aufgabe an.

Tag

Gibt den eindeutigen Bezeichner für die Aufgabe an. Dieser wird in URLs, Webservices bzw. Eigenschaftendateien verwendet. Er muss aus Buchstaben, Zahlen oder Unterstrichen bestehen und mit einem Buchstaben oder einem Unterstrich beginnen.

Registerkarte ausblenden

Gibt an, dass die Registerkarte den Benutzern angezeigt, jedoch nicht ausgeführt wird. Wenn Sie diese Option auswählen, wird den Benutzern in CA IdentityMinder ein Fehler angezeigt.

Aufgabenliste beim Laden anzeigen

Zeigt die Aufgaben an, die für den aktuellen Tag übermittelt wurden.

Hinweis: Wenn diese Option aktiviert ist, werden den Benutzern beim Klicken auf "Übermittelte Aufgaben anzeigen" direkt die Aufgaben angezeigt, die am gleichen Tag übermittelt wurden.

Überwachungsereignisse anzeigen

Gibt an, ob überwachte Ereignisse in den Aufgaben auf der Seite "Übermittelte Aufgaben anzeigen" enthalten sind.

Benutzerdefinierte Spalte zulassen

Gibt an, dass an die Aufgabentabelle eine benutzerdefinierte Spalte angehängt werden kann, die auf der Registerkarte "Übermittelte Aufgaben anzeigen" und "Benutzerverlauf" angezeigt werden kann. Sie können beispielsweise die Spalte "Benutzer-ID" an die Aufgabentabelle anhängen, die auf der Registerkarte "Benutzerverlauf" angezeigt wird.

Überschrift der benutzerdefinierten Spalte

Gibt den Anzeigenamen der benutzerdefinierten Spalte an.

Attribut für benutzerdefinierte Spalte

Gibt das Attribut an, das zum Füllen der benutzerdefinierten Spalte in der Aufgabentabelle verwendet wird. Falls Sie beispielsweise nach Aufgaben suchen, die für Arbeitnehmer einer Organisation ausgeführt werden, können Sie eine Organisationsspalte anhängen, in der die Organisation eines jeden Arbeitnehmers angezeigt wird.

Aufgaben und Ereignisse abbrechen

Gibt die Kriterien zum Abbrechen von Aufgaben oder Ereignissen an. Sie können den Bereich für dieses Feld festlegen, indem Sie eine der folgenden Optionen auswählen:

Aufgabenersteller muss der aktuelle Benutzer sein

Gibt an, dass Sie erneut gesendete Aufgaben oder Ereignisse abbrechen können, die Sie erstellt haben.

Aufgabenersteller muss im Gültigkeitsbereich sein

Gibt an, dass Sie erneut gesendete Aufgaben oder Ereignisse abbrechen können, die von anderen Benutzern initiiert wurden, die mit den Benutzerbereichsregeln für die Admin-Rolle übereinstimmen, über die Sie Zugriff auf die Registerkarte haben.

Ihnen wurde beispielsweise die Rolle "Benutzer-Manager" zugeteilt, die die Option "Übermittelte Aufgaben anzeigen" enthält, da Sie mit den Kriterien in einer Mitgliedschaftsregel übereinstimmen, die den Bereich aller Benutzer in der Organisation "Arbeitnehmer" enthält. Sie können Aufgaben abbrechen oder erneut senden, die von allen Benutzern in der Organisation "Arbeitnehmer" übermittelt wurden.

Keine Einschränkungen

Gibt an, dass alle Benutzer Aufgaben oder Ereignisse abbrechen oder erneut senden können.

Nicht erlaubt

Gibt an, dass Aufgaben oder Ereignisse nicht abgebrochen oder erneut gesendet werden können.

Aufgaben und Ereignisse erneut senden

Gibt die Kriterien zum erneuten Senden von Aufgaben oder Ereignissen an. Sie können den Bereich dieses Felds festlegen, indem Sie eine der folgenden Optionen auswählen:

Aufgabenersteller muss der aktuelle Benutzer sein

Gibt an, dass Sie erneut gesendete Aufgaben oder Ereignisse abbrechen können, die Sie erstellt haben.

Aufgabenersteller muss im Gültigkeitsbereich sein

Gibt an, dass Sie erneut gesendete Aufgaben oder Ereignisse abbrechen können, die von anderen Benutzern initiiert wurden, die mit den Benutzerbereichsregeln für die Admin-Rolle übereinstimmen, über die Sie Zugriff auf die Registerkarte haben.

Ihnen wurde beispielsweise die Rolle "Benutzer-Manager" zugeteilt, die die Option "Übermittelte Aufgaben anzeigen" enthält, da Sie mit den Kriterien in einer Mitgliedschaftsregel übereinstimmen, die den Bereich aller Benutzer in der Organisation "Arbeitnehmer" enthält. Sie können Aufgaben abbrechen oder erneut senden, die von allen Benutzern in der Organisation "Arbeitnehmer" übermittelt wurden.

Keine Einschränkungen

Gibt an, dass alle Benutzer Aufgaben oder Ereignisse abbrechen oder erneut senden können.

Nicht erlaubt

Gibt an, dass Aufgaben oder Ereignisse nicht abgebrochen oder erneut gesendet werden können.

Registerkarte "Benutzerverlauf"

Die Registerkarte "Benutzerverlauf" ermöglicht es Ihnen, Aufgaben anzuzeigen, die sich auf einen Benutzer beziehen. Die Aufgabendetails, die auf dieser Registerkarte angezeigt werden, können auch auf der Registerkarte "Gesendete Aufgaben anzeigen" angezeigt werden.

Hinweis: Sie können diese Registerkarte nicht zu den Erstellungsaufgaben, wie z. B. "Benutzer erstellen", hinzufügen.

Sie können diese Registerkarte verwenden, um einen Verlauf der folgenden Aufgaben anzuzeigen:

- **Aufgaben, die für den Benutzer durchgeführt wurden**

  Zeigt alle Aufgaben an, die für den ausgewählten Benutzer durchgeführt werden.

- **Aufgaben, die vom Benutzer durchgeführt wurden**

  Zeigt alle Aufgaben an, die vom ausgewählten Benutzer durchgeführt werden.

- **Workflow-Genehmigung dieses Benutzers**

  Zeigt alle Aufgaben an, die der Benutzer als Teil eines Workflow genehmigt hat.

Hinweis: Der Typ der Aufgaben, die Sie auf dieser Registerkarte anzeigen können, hängt von der Konfiguration der Registerkarte ab. Weitere Informationen finden Sie unter Anpassen der Registerkarte "Benutzerverlauf" (siehe Seite 596).

Suchattribute zum Anzeigen des Benutzerverlaufs

Um Aufgaben zu überprüfen, die zur Verarbeitung übermittelt wurden, können Sie die Suchfunktion in "Übermittelte Aufgaben anzeigen" verwenden. Sie können basierend auf folgenden Kriterien nach Aufgaben suchen:

Aufgabenname

Gibt den Aufgabennamen als Suchkriterium an. Sie können die Suche mit dem Wert des Felds "Mit Aufgabennamen" verfeinern, indem Sie Bedingungen wie "gleich", "enthält", "startet mit" oder "endet auf" angeben. Sie können beispielsweise das Suchkriterium "Aufgabenname gleich Benutzer erstellen" angeben, indem Sie die Bedingung "gleich" auswählen und im Textfeld "Benutzer erstellen" eingeben.

Aufgabenstatus

Gibt den Aufgabenstatus als Suchkriterium an. Sie können den Aufgabenstatus auswählen, indem Sie "Mit Aufgabenstatus gleich" aktivieren und die Bedingung auswählen. Basierend auf den folgenden Bedingungen können Sie die Suche noch weiter verfeinern:

- Abgeschlossen
- In Bearbeitung
- Fehlgeschlagen
- Abgelehnt
- Teilweise abgeschlossen
- Abgebrochen
- Geplant

Hinweis: Weitere Informationen finden Sie unter Beschreibungen des Aufgabenstatus (siehe Seite 587).

Aufgabenpriorität

Gibt die Aufgabenpriorität als Suchkriterium an. Sie können die Aufgabenpriorität auswählen, indem Sie "Mit Aufgabenpriorität gleich" aktivieren und die Bedingung auswählen. Basierend auf den folgenden Bedingungen können Sie die Suche noch weiter verfeinern:

Niedrig

Gibt an, dass Sie nach Aufgaben mit der Priorität "Niedrig" suchen können.

Mittel

Gibt an, dass Sie nach Aufgaben mit der Priorität "Mittel" suchen können.

Hoch

Gibt an, dass Sie nach Aufgaben mit der Priorität "Hoch" suchen können.

Datumsbereich

Gibt die Daten an, innerhalb derer Sie nach übermittelten Aufgaben suchen möchten. Sie müssen das Start- und Enddatum angeben.

Anpassen der Registerkarte "Benutzerverlauf"

Administratoren können die Registerkarte "Benutzerverlauf" wie folgt anpassen:

- Angeben eines anderen Aufgabennamens und -tags.
- Ändern der standardmäßigen Anzeigeeigenschaften. Standardmäßig können Benutzer Kriterien eingeben, die bestimmen, welche Aufgaben auf der Registerkarte angezeigt werden. Administratoren können die Registerkarte so konfigurieren, dass automatisch die Aufgaben des aktuellen Tages angezeigt werden, sodass die Benutzer keine Suchkriterien mehr eingeben müssen.

- Festlegen, ob Überwachungsereignisse auf der Seite "Aufgabendetails" angezeigt werden.
- Hinzufügen einer Spalte zur Aufgabenanzeige.
- Angeben der Kriterien zum Abbrechen oder erneuten Senden von Aufgaben und Ereignissen.

Gehen Sie wie folgt vor:

1. Wählen Sie die Optionen "Rollen und Aufgaben", "Admin-Aufgaben", "Admin-Aufgabe ändern" aus.

   Daraufhin wird die Seite "Admin-Aufgabe auswählen" angezeigt.

2. Wählen Sie im Feld "Admin-Aufgaben durchsuchen" die Option "Name" oder "Kategorie" aus, geben Sie die zu suchende Zeichenfolge ein, und klicken Sie dann auf "Suchen".

   Daraufhin werden in CA IdentityMinder die Admin-Aufgaben angezeigt, die den Suchkriterien entsprechen.

3. Wählen Sie die Aufgabe mit der Registerkarte "Benutzerverlauf" aus, und klicken Sie auf "Auswählen".

   In CA IdentityMinder werden die Aufgabendetails der Admin-Aufgabe angezeigt.

4. Klicken Sie auf die Registerkarte "Registerkarten".

5. Klicken Sie auf das Bearbeitungssymbol neben der Registerkarte "Benutzerverlauf".

   Die Registerkartendetails werden angezeigt.

6. Bearbeiten Sie die Felder, um die Registerkarte "Benutzerverlauf" anzupassen.

   Informationen

Konfigurationseinstellungen der Registerkarte "Benutzerverlauf"

Verwenden Sie die folgenden Felder, um die Darstellung und die Funktionen der Registerkarte "Benutzerverlauf" zu ändern.

Name

Gibt den Namen der Aufgabe an.

Tag

Gibt den eindeutigen Bezeichner für die Aufgabe an. Dieser wird in URLs, Webservices bzw. Eigenschaftendateien verwendet. Er muss aus Buchstaben, Zahlen oder Unterstrichen bestehen und mit einem Buchstaben oder einem Unterstrich beginnen.

Registerkarte ausblenden

Gibt an, dass die Registerkarte den Benutzern angezeigt, jedoch nicht ausgeführt wird. Wenn Sie diese Option auswählen, wird den Benutzern in CA IdentityMinder ein Fehler angezeigt.

Aufgabenliste beim Laden anzeigen

Zeigt die Aufgaben an, die für den aktuellen Tag übermittelt wurden.

Hinweis: Wenn diese Option aktiviert ist, werden den Benutzern beim Klicken auf "Übermittelte Aufgaben anzeigen" direkt die Aufgaben angezeigt, die am gleichen Tag übermittelt wurden.

Überwachungsereignisse anzeigen

Gibt an, ob überwachte Ereignisse in den Aufgaben auf der Seite "Übermittelte Aufgaben anzeigen" enthalten sind.

Benutzerdefinierte Spalte zulassen

Gibt an, dass an die Aufgabentabelle eine benutzerdefinierte Spalte angehängt werden kann, die auf der Registerkarte "Übermittelte Aufgaben anzeigen" und "Benutzerverlauf" angezeigt werden kann. Sie können beispielsweise die Spalte "Benutzer-ID" an die Aufgabentabelle anhängen, die auf der Registerkarte "Benutzerverlauf" angezeigt wird.

Überschrift der benutzerdefinierten Spalte

Gibt den Anzeigenamen der benutzerdefinierten Spalte an.

Attribut für benutzerdefinierte Spalte

Gibt das Attribut an, das zum Füllen der benutzerdefinierten Spalte in der Aufgabentabelle verwendet wird. Falls Sie beispielsweise nach Aufgaben suchen, die für Arbeitnehmer einer Organisation ausgeführt werden, können Sie eine Organisationsspalte anhängen, in der die Organisation eines jeden Arbeitnehmers angezeigt wird.

Aufgaben und Ereignisse abbrechen

Gibt die Kriterien zum Abbrechen von Aufgaben oder Ereignissen an. Sie können den Bereich für dieses Feld festlegen, indem Sie eine der folgenden Optionen auswählen:

Aufgabenersteller muss der aktuelle Benutzer sein

Gibt an, dass Sie erneut gesendete Aufgaben oder Ereignisse abbrechen können, die Sie erstellt haben.

Aufgabenersteller muss im Gültigkeitsbereich sein

Gibt an, dass Sie erneut gesendete Aufgaben oder Ereignisse abbrechen können, die von anderen Benutzern initiiert wurden, die mit den Benutzerbereichsregeln für die Admin-Rolle übereinstimmen, über die Sie Zugriff auf die Registerkarte haben.

Ihnen wurde beispielsweise die Rolle "Benutzer-Manager" zugeteilt, die die Option "Übermittelte Aufgaben anzeigen" enthält, da Sie mit den Kriterien in einer Mitgliedschaftsregel übereinstimmen, die den Bereich aller Benutzer in der Organisation "Arbeitnehmer" enthält. Sie können Aufgaben abbrechen oder erneut senden, die von allen Benutzern in der Organisation "Arbeitnehmer" übermittelt wurden.

Keine Einschränkungen

Gibt an, dass alle Benutzer Aufgaben oder Ereignisse abbrechen oder erneut senden können.

Nicht erlaubt

Gibt an, dass Aufgaben oder Ereignisse nicht abgebrochen oder erneut gesendet werden können.

Aufgaben und Ereignisse erneut senden

Gibt die Kriterien zum erneuten Senden von Aufgaben oder Ereignissen an. Sie können den Bereich dieses Felds festlegen, indem Sie eine der folgenden Optionen auswählen:

Aufgabenersteller muss der aktuelle Benutzer sein

Gibt an, dass Sie erneut gesendete Aufgaben oder Ereignisse abbrechen können, die Sie erstellt haben.

Aufgabenersteller muss im Gültigkeitsbereich sein

Gibt an, dass Sie erneut gesendete Aufgaben oder Ereignisse abbrechen können, die von anderen Benutzern initiiert wurden, die mit den Benutzerbereichsregeln für die Admin-Rolle übereinstimmen, über die Sie Zugriff auf die Registerkarte haben.

Ihnen wurde beispielsweise die Rolle "Benutzer-Manager" zugeteilt, die die Option "Übermittelte Aufgaben anzeigen" enthält, da Sie mit den Kriterien in einer Mitgliedschaftsregel übereinstimmen, die den Bereich aller Benutzer in der Organisation "Arbeitnehmer" enthält. Sie können Aufgaben abbrechen oder erneut senden, die von allen Benutzern in der Organisation "Arbeitnehmer" übermittelt wurden.

Keine Einschränkungen

Gibt an, dass alle Benutzer Aufgaben oder Ereignisse abbrechen oder erneut senden können.

Nicht erlaubt

Gibt an, dass Aufgaben oder Ereignisse nicht abgebrochen oder erneut gesendet werden können.

Aufgaben anzeigen

Legt die Aufgaben fest, die auf der Registerkarte "Benutzerverlauf" angezeigt werden.

Aufgaben, die für den Benutzer durchgeführt wurden

Zeigt alle Aufgaben an, die für den Benutzer durchgeführt wurden.

Aufgaben, die vom Benutzer durchgeführt wurden

Zeigt alle Aufgaben an, die vom Benutzer durchgeführt wurden.

Workflow-Genehmigung dieses Benutzers

Zeigt alle Aufgaben an, die der Benutzer als Teil eines Workflow genehmigt hat.

Die Aufgabe "Benutzeraktivität anzeigen"

Bei der Benutzeraktivität handelt es sich um den Aufgabenverlauf eines bestimmten Benutzers. Administratoren können die Aufgabe "Benutzeraktivität anzeigen" verwenden, um die folgenden Benutzerinformationen zu verfolgen:

- Aufgaben, die für den Benutzer durchgeführt wurden
- Aufgaben, die vom Benutzer durchgeführt wurden
- Workflow-Genehmigung, die vom Benutzer durchgeführt wurden

So zeigen Sie die Benutzeraktivität an:

1. Klicken Sie auf die Optionen "Benutzer", "Benutzer verwalten", "Benutzeraktivität anzeigen".

   Das Fenster "Benutzer auswählen" wird angezeigt.

2. Suchen Sie nach einem Benutzer und klicken Sie auf "Auswählen".

   Das Fenster "Benutzeraktivität anzeigen" wird angezeigt.

Hinweis: Weitere Informationen zur angezeigten Benutzeraktivität finden Sie in der Online-Hilfe zur Benutzerkonsole.

Bereinigen gesendeter Aufgaben

Mit jeder gesendeten Aufgabe wächst die Aufgaben-Persistenz-Datenbank. Dadurch nimmt die Leistung der Aufgaben und Ereignisse zur Laufzeit ab. Die Bereinigung von "Stored Procedures" reduziert die Wahrscheinlichkeit von Leistungsproblemen oder Systemausfällen, die durch Speicherplatzmangel der Aufgaben-Persistenz-Datenbank entstehen können. Der Administrator kann die Aufgaben archivieren und ist daher auch in der Lage, eine Ansicht mit den Informationen zur aktuellen Aufgabe, Ereignisinformationen sowie gelöschte Aufgaben und Ereignisse aufzurufen.

CA IdentityMinder-Administratoren können Jobs in der Benutzerkonsole planen, die regelmäßig eine automatische Bereinigung und Archivierung durchführen.

Registerkarte "Wiederholungen"

Planen Sie Ihren Job auf dieser Registerkarte. Diese Registerkarte enthält die folgenden Felder:

Jetzt ausführen

Führt den Job sofort aus.

Neuen Job planen

Plant einen neuen Job.

Vorhandenen Job ändern

Gibt an, dass Sie einen bereits vorhandenen Job ändern möchten.

Hinweis: Dieses Feld wird nur angezeigt, wenn ein Job bereits für diese Aufgabe geplant wurde.

Jobname

Gibt den Namen des Jobs an, den Sie erstellen oder ändern möchten.

Zeitzone

Gibt die Serverzeitzone an.

Hinweis: Wenn Ihre Zeitzone sich von der Zeitzone des Servers unterscheidet, wird beim Planen eines neuen Jobs eine Dropdown-Liste angezeigt, damit Sie entweder Ihre Zeitzone oder die Zeitzone Ihres Servers auswählen können. Sie können die Zeitzone beim Ändern eines vorhandenen Jobs nicht anpassen.

Täglicher Ablaufplan

Gibt an, dass der Job immer nach einer bestimmten Anzahl von Tagen ausgeführt wird.

Alle (Anzahl der Tage)

Definiert, wie viele Tage zwischen den Jobausführungen liegen.

Wöchentlicher Ablaufplan

Gibt an, dass der Job an einem bestimmten Tag bzw. bestimmten Tagen und zu einem bestimmten Zeitpunkt in der Woche ausgeführt wird.

Wochentag

Legt den Tag bzw. die Tage in der Woche fest, an dem bzw. denen der Job ausgeführt wird.

Monatlicher Ablaufplan

Legt einen Tag der Woche oder des Monats fest, an dem der Job monatlich ausgeführt wird.

Jährlicher Ablaufplan

Legt einen Tag der Woche oder des Monats fest, an dem der Job jährlich ausgeführt wird.

Erweiterter Ablaufplan

Legt zusätzliche Zeitplaninformationen fest.

Cron-Ausdruck

Informationen zum Ausfüllen dieses Feldes finden Sie unter

http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html

Ausführungszeit

Gibt die Tageszeit zum Ausführen des Jobs im 24-Stunden-Format an. Beispiel: 14:15.

Sofortiges Ausführen eines Jobs

Verwenden Sie zum sofortigen Ausführen eines Jobs den Assistenten "Gesendete Aufgaben bereinigen" sofort aus.

Gehen Sie in der Registerkarte "System" wie folgt vor:

1. Wählen Sie im linken Fensterbereich "Gesendete Aufgaben bereinigen" aus.

   Der Schritt "Wiederholungen" des Assistenten wird angezeigt.

2. Wählen Sie "Jetzt ausführen" und anschließend "Weiter".

   Der Schritt "Gesendete Aufgaben bereinigen" des Assistenten wird angezeigt.

3. Geben Sie Informationen zu Mindestalter, Archiv, Zeitlimit für die Überprüfung, Zeitlimit und Aufgabenlimit ein, und klicken Sie auf "Fertig stellen".

   Der Job wird sofort gesendet.

Planen eines neuen Jobs

Planen Sie einen neuen Job mit Hilfe des Assistenten "Gesendete Aufgaben bereinigen".

Gehen Sie in der Registerkarte "System" wie folgt vor:

1. Wählen Sie im linken Fensterbereich "Gesendete Aufgaben bereinigen" aus.

   Der Schritt "Wiederholungen" wird angezeigt.

2. Wählen Sie "Neuen Job planen", geben Sie den Jobnamen und Zeitplaninformationen für den Job ein, und klicken Sie auf "Weiter".

   Der Schritt "Gesendete Aufgaben bereinigen" wird angezeigt.

3. Geben Sie Informationen zu Mindestalter, Archiv, Zeitlimit für die Überprüfung, Zeitlimit und Aufgabenlimit ein, und klicken Sie auf "Fertig stellen".

   Der neue Job wurde geplant.

Ändern eines vorhandenen Jobs

Verwenden Sie zum Ändern einens vorhandenen Jobs den Assistenten "Gesendete Aufgaben bereinigen".

Gehen Sie in der Registerkarte "System" wie folgt vor:

1. Wählen Sie im linken Fensterbereich "Gesendete Aufgaben bereinigen" aus.

   Der Schritt "Wiederholungen" wird angezeigt.

2. Klicken Sie auf "Vorhandenen Job ändern", und wählen Sie einen vorhandenen Job aus, ändern Sie die Zeitplaninformationen, und klicken Sie auf "Weiter".

   Der Schritt "Gesendete Aufgaben bereinigen" wird angezeigt.

3. Ändern Sie Mindestalter, Archiv, Zeitlimit für die Überprüfung, Zeitlimit und Aufgabenlimit nach Bedarf, und klicken Sie auf "Fertig stellen".

   Der vorhandene Job wird geändert.

Löschen einer wiederkehrenden Aufgabe

Gehen Sie zum Löschen einer wiederkehrenden Aufgabe folgendermaßen vor:

In "Gesendete Aufgaben anzeigen"

1. wählen Sie "Wiederkehrende Aufgabe löschen".
2. Wählen Sie die Aufgabe aus, die Sie löschen möchten.
3. Klicken Sie auf "Senden".

Registerkarte "Gesendete Aufgaben bereinigen"

Legen Sie Mindestalter, Archiv, Zeitlimit für die Überprüfung, Zeitlimit und Aufgabenlimit der Aufgabe auf dieser Registerkarte fest. Klicken Sie nach dem Ausfüllen der Pflichtfelder auf "Fertig stellen". Diese Registerkarte enthält die folgenden Felder:

Mindestalter

Legt das Mindestalter fest, das abgeschlossene, fehlgeschlagene, abgelehnte oder abgebrochene Aufgaben haben müssen, damit sie bereinigt werden. Wenn Sie beispielsweise einen Monat angegeben haben, werden alle Aufgaben beibehalten, die im letzten Monat abgeschlossen wurden. Alle Aufgaben, die vor mehr als einem Monat abgeschlossen wurden, werden bereinigt und archiviert.

Dieses Feld ist erforderlich.

Archivieren

Sichert Aufgaben in der Archivdatenbank, und löscht sie anschließend aus der Laufzeitdatenbank.

Wenn der Job ausgeführt und "Archivieren" aktiviert ist, werden die Daten an die Archivdatenbank übergeben und aus der Laufzeit-Aufgaben-Persistenz-Datenbank entfernt. Die Daten werden solange nicht entfernt, bis eine erfolgreiche Festschreibung auf die Archivdatenbank erfolgt.

Zeitlimit für die Überprüfung

Legt den Zeitraum vor dem Bereinigen der Aufgaben im Überprüfungsstatus fest. Aufgaben im Überprüfungsstatus gelten vor Ende dieses Zeitraums nicht als abgeschlossen. Die Aufgaben im Überprüfungsstatus wurden nicht gesendet.

Zeitlimit

Beschränkt die Bereinigung auf einen bestimmten Zeitraum.

Aufgabenlimit

Beschränkt die Bereinigung auf eine bestimmte Anzahl von Aufgaben.

Löschen wiederkehrender Aufgaben

Wenn eine Aufgabe nicht mehr regelmäßig ausgeführt werden muss, kann der CA IdentityMinder-Administrator die Aufgabe löschen. Nach dem Löschen der Aufgabe wird sie weder bereinigt noch archiviert.

Alle mit Hilfe des Assistenten "Gesendete Aufgaben bereinigen" geplanten Aufgaben sind auf der Seite "Wiederholungen" aufgeführt. Der CA IdentityMinder-Administrator kann die zu löschende Aufgaben auswählen.

Hinweis: Die Aufgaben befinden sich weiterhin in der Datenbank, es werden nur die geplanten Wiederholungen gelöscht.

Konfigurieren der Enterprise Log Manager-Verbindung

Verwenden Sie dieses Fenster, um neu hinzugefügte CA User Activity Reporting (CA UAR)-Verbindungsaufgaben zu verwalten.

Hinweis: CA Enterprise Log Manager ist umbenannt worden in CA-UAR.

Dieses Fenster enthält folgende Felder:

Verbindungsname

Gibt den eindeutigen Namen an, der für das einzelne verwaltete CA-UAR-Verbindungsobjekt verwendet wird.

Dieses Feld ist schreibgeschützt.

Beschreibung

Beschreibt die CA-UAR-Verbindung.

Hostname

Gibt den Hostnamen oder die IP-Adresse des CA-UAR-Servers an.

Dieses Feld ist erforderlich.

Port-Nr.

Gibt den CA-UAR-Serververbindungsport an.

Standard: 52520

Dieses Feld ist erforderlich.

Von einer Zertifizierungsstelle unterzeichnetes SSL-Zertifikat

Wenn dieses Kontrollkästchen aktiviert ist, wird eine strikte SSL-Zertifikatsprüfung bei der Herstellung einer Verbindung mit einem CA-UAR-Server durchgeführt.

Wenn Sie über ein selbst signiertes SSL-Zertifikat verfügen, z. B. ein standardmäßig mit CA-UAR installiertes Zertifikat, darf dieses Kontrollkästchen nicht aktiviert werden, da kein vertrauenswürdiger Pfad zur Root Certificate Authority vorhanden ist.

Zertifikatsname

Gibt den Namen des für die Authentifizierung zu verwendenden CA-UAR-Zertifikats an.

Dieses Feld ist erforderlich.

Zertifizierungskennwort

Gibt das CA-UAR-Kennwort an.

Dieses Feld ist erforderlich.

Attribut

Nicht unterstützt. Die Version wird abgerufen, wenn das Speichern von Verbindungsinformationen versucht wird.

Löschen der Enterprise Log Manager-Verbindung

Wählen Sie eine Verbindung aus der Liste aus, und klicken Sie auf "Löschen". Die CA-UAR-Verbindung wird gelöscht.

Geheime Schlüssel verwalten

Verwenden Sie geheime Schlüssel, um dynamische Schlüssel zu verwalten, die Daten verschlüsseln oder entschlüsseln. Wenn Sie vermuten, dass ein Benutzer unbefugten Zugriff auf einen Schlüssel erhalten hat, können Sie das Kennwort für den Schlüsselspeicher ändern. Der Schlüsselspeicher ist die Datenbank für geheime Schlüssel. Sobald Sie dieses Kennwort ändern, verschlüsselt CA IdentityMinder die Werte der Schlüssel wieder.

Jede Umgebung verfügt über einen Satz mit dynamischen Schlüsseln und einem Schlüsselspeicherkennwort. Wenn Umgebungen ein Benutzerverzeichnis gemeinsam nutzen, verwenden Sie die gleichen dynamischen Schlüssel und das gleiche Schlüsselspeicherkennwort für jede Umgebung.

Kennwörter des Schlüsselspeichers werden mithilfe von in Verschlüsselungscode eingebetteten Schlüsseln oder während der Installation des CA IdentityMinder-Servers eingegebenen Parametern verschlüsselt. In einem Cluster nutzen alle Knoten die Werte für dynamische Schlüssel und das Schlüsselspeicherkennwort gemeinsam.

Verschlüsselungsvorgänge verwenden den letzten dynamischen Schlüssel für den entsprechenden Algorithmus und die entsprechende Umgebung. Entschlüsselungsvorgänge überprüfen, ob eine Schlüssel-ID in den verschlüsselten Daten vorhanden ist, damit der richtige Schlüssel verwendet wird. Ausführliche Informationen finden Sie im Abschnitt Encrypted Text Formats im *Konfigurationshandbuch*.

Gehen Sie wie folgt vor:

1. Geben Sie das Kennwort für den Schlüsselspeicher ein, oder ändern Sie es.
2. Klicken Sie auf "Schlüssel hinzufügen", wenn Sie einen anderen Schlüssel benötigen.
3. Wählen Sie einen Algorithmus aus.
4. Geben Sie ein Kennwort für den Schlüssel ein.

   Für PBE und RC2 ist die größtmögliche Schlüssellänge 128 Byte.

   Für AES sind die gültigen Schlüsselgrößen 16, 24 und 32 Byte.
5. Klicken Sie auf "Senden".
6. Wenn Sie das Schlüsselspeicher-Kennwort geändert haben, klicken Sie auf "Senden".

   CA IdentityMinder verschlüsselt erneut die Werte der Schlüssel.

Kapitel 21: Aufgabenpersistenz

Dieses Kapitel enthält folgende Themen:

Automatisierte Aufgaben-Persistenz-Bereinigung und -Archivierung (siehe Seite 609)
Registerkarte "Wiederholungen" (siehe Seite 610)
Registerkarte "Gesendete Aufgaben bereinigen" (siehe Seite 611)
Sofortiges Ausführen eines Jobs (siehe Seite 612)
Planen eines neuen Jobs (siehe Seite 612)
Ändern eines vorhandenen Jobs (siehe Seite 613)
Löschen einer wiederkehrenden Aufgabe (siehe Seite 613)
Migrieren der Aufgabenpersistenz-Datenbank (siehe Seite 614)

Automatisierte Aufgaben-Persistenz-Bereinigung und -Archivierung

In dieser Ausgabe kann ein Administrator Jobs mit spezifischen Parametern unter Verwendung des Tasks "Gesendete Aufgaben bereinigen" planen und verändern, um Aufgaben- und Ereignisinformationen in der Aufgaben-Persistenz-Datenbank zu bereinigen und zu archivieren und wiederkehrende Aufgaben wie diese nach Bedarf zu löschen.

In der Registerkarte "System" können Sie über die Option "Bereinigen gesendeter Aufgaben" einen Assistenten starten. Von dort aus führt Sie der Assistent durch Aufgabeneinstellungen und -planungen und fragt Sie, ob Sie die Daten archivieren möchten oder nicht. Sie können bei Bedarf die wiederkehrenden Aufgaben auch löschen, indem Sie die System-Registerkartenoption "Löschen wiederkehrender Aufgaben" auswählen.

Indem Sie die Aufgabenbereinigungs- und Datenarchivierung-Tasks planen, reduzieren Sie die Wahrscheinlichkeit für das Auftreten von Leistungsproblemen oder Systemausfällen deutlich. Über die Archivierungsfunktion können Sie die Aufgaben auf der Archivdatenbank sichern, bevor Sie sie von der Laufzeitdatenbank löschen. Wenn Sie die gelöschten Aufgaben nochmals ansehen möchten, markieren Sie das Kontrollkästchen "Archiv gesendeter Aufgaben durchsuchen" unter "Gesendete Aufgeben anzeigen", um eine Liste aller Aufgaben zu suchen und anzuzeigen, die gelöscht und archiviert wurden.

Registerkarte "Wiederholungen"

Planen Sie Ihren Job auf dieser Registerkarte. Diese Registerkarte enthält die folgenden Felder:

Jetzt ausführen

Führt den Job sofort aus.

Neuen Job planen

Plant einen neuen Job.

Vorhandenen Job ändern

Gibt an, dass Sie einen bereits vorhandenen Job ändern möchten.

Hinweis: Dieses Feld wird nur angezeigt, wenn ein Job bereits für diese Aufgabe geplant wurde.

Jobname

Gibt den Namen des Jobs an, den Sie erstellen oder ändern möchten.

Zeitzone

Gibt die Serverzeitzone an.

Hinweis: Wenn Ihre Zeitzone sich von der Zeitzone des Servers unterscheidet, wird beim Planen eines neuen Jobs eine Dropdown-Liste angezeigt, damit Sie entweder Ihre Zeitzone oder die Zeitzone Ihres Servers auswählen können. Sie können die Zeitzone beim Ändern eines vorhandenen Jobs nicht anpassen.

Wöchentlicher Ablaufplan

Gibt an, dass der Job an einem bestimmten Tag bzw. bestimmten Tagen und zu einem bestimmten Zeitpunkt in der Woche ausgeführt wird.

Erweiterter Ablaufplan

Legt zusätzliche Zeitplaninformationen fest.

Wochentag

Legt den Tag bzw. die Tage in der Woche fest, an dem der Job ausgeführt wird.

Ausführungszeit

Gibt die Tageszeit zum Ausführen des Jobs im 24-Stunden-Format an. Beispiel: 14:15.

Cron-Ausdruck

Informationen zum Ausfüllen dieses Feldes finden Sie unter

"http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html"

Hinweis: Dieses Feld wird angezeigt, wenn "Erweiterter Ablaufplan" ausgewählt wird.

Weitere Informationen:

Löschen einer wiederkehrenden Aufgabe (siehe Seite 603)
Planen eines neuen Jobs (siehe Seite 603)
Ändern eines vorhandenen Jobs (siehe Seite 603)
Sofortiges Ausführen eines Jobs (siehe Seite 602)

Registerkarte "Gesendete Aufgaben bereinigen"

Legen Sie Mindestalter, Archiv, Zeitlimit für die Überprüfung, Zeitlimit und Aufgabenlimit der Aufgabe auf dieser Registerkarte fest. Klicken Sie nach dem Ausfüllen der Pflichtfelder auf "Fertig stellen". Diese Registerkarte enthält die folgenden Felder:

Mindestalter

Legt das Mindestalter fest, das abgeschlossene, fehlgeschlagene, abgelehnte oder abgebrochene Aufgaben haben müssen, damit sie bereinigt werden. Wenn Sie beispielsweise einen Monat angegeben haben, werden alle Aufgaben beibehalten, die im letzten Monat abgeschlossen wurden. Alle Aufgaben, die vor mehr als einem Monat abgeschlossen wurden, werden bereinigt und archiviert.

Dieses Feld ist erforderlich.

Archivieren

Sichert Aufgaben in der Archivdatenbank, und löscht sie anschließend aus der Laufzeitdatenbank.

Wenn der Job ausgeführt und "Archivieren" aktiviert ist, werden die Daten an die Archivdatenbank übergeben und aus der Laufzeit-Aufgaben-Persistenz-Datenbank entfernt. Die Daten werden solange nicht entfernt, bis eine erfolgreiche Festschreibung auf die Archivdatenbank erfolgt.

Zeitlimit für die Überprüfung

Legt den Zeitraum vor dem Bereinigen der Aufgaben im Überprüfungsstatus fest. Aufgaben im Überprüfungsstatus gelten vor Ende dieses Zeitraums nicht als abgeschlossen. Die Aufgaben im Überprüfungsstatus wurden nicht gesendet.

Zeitlimit

Beschränkt die Bereinigung auf einen bestimmten Zeitraum.

Aufgabenlimit

Beschränkt die Bereinigung auf eine bestimmte Anzahl von Aufgaben.

Sofortiges Ausführen eines Jobs

Verwenden Sie zum sofortigen Ausführen eines Jobs den Assistenten "Gesendete Aufgaben bereinigen" sofort aus.

Gehen Sie in der Registerkarte "System" wie folgt vor:

1. Wählen Sie im linken Fensterbereich "Gesendete Aufgaben bereinigen" aus.

   Der Schritt "Wiederholungen" des Assistenten wird angezeigt.

2. Wählen Sie "Jetzt ausführen" und anschließend "Weiter".

   Der Schritt "Gesendete Aufgaben bereinigen" des Assistenten wird angezeigt.

3. Geben Sie Informationen zu Mindestalter, Archiv, Zeitlimit für die Überprüfung, Zeitlimit und Aufgabenlimit ein, und klicken Sie auf "Fertig stellen".

   Der Job wird sofort gesendet.

Planen eines neuen Jobs

Planen Sie einen neuen Job mit Hilfe des Assistenten "Gesendete Aufgaben bereinigen".

Gehen Sie in der Registerkarte "System" wie folgt vor:

1. Wählen Sie im linken Fensterbereich "Gesendete Aufgaben bereinigen" aus.

   Der Schritt "Wiederholungen" wird angezeigt.

2. Wählen Sie "Neuen Job planen", geben Sie den Jobnamen und Zeitplaninformationen für den Job ein, und klicken Sie auf "Weiter".

   Der Schritt "Gesendete Aufgaben bereinigen" wird angezeigt.

3. Geben Sie Informationen zu Mindestalter, Archiv, Zeitlimit für die Überprüfung, Zeitlimit und Aufgabenlimit ein, und klicken Sie auf "Fertig stellen".

   Der neue Job wurde geplant.

Ändern eines vorhandenen Jobs

Verwenden Sie zum Ändern einens vorhandenen Jobs den Assistenten "Gesendete Aufgaben bereinigen".

Gehen Sie in der Registerkarte "System" wie folgt vor:

1. Wählen Sie im linken Fensterbereich "Gesendete Aufgaben bereinigen" aus.

   Der Schritt "Wiederholungen" wird angezeigt.

2. Klicken Sie auf "Vorhandenen Job ändern", und wählen Sie einen vorhandenen Job aus, ändern Sie die Zeitplaninformationen, und klicken Sie auf "Weiter".

   Der Schritt "Gesendete Aufgaben bereinigen" wird angezeigt.

3. Ändern Sie Mindestalter, Archiv, Zeitlimit für die Überprüfung, Zeitlimit und Aufgabenlimit nach Bedarf, und klicken Sie auf "Fertig stellen".

   Der vorhandene Job wird geändert.

Löschen einer wiederkehrenden Aufgabe

Gehen Sie zum Löschen einer wiederkehrenden Aufgabe folgendermaßen vor:

In "Gesendete Aufgaben anzeigen"

1. wählen Sie "Wiederkehrende Aufgabe löschen".
2. Wählen Sie die Aufgabe aus, die Sie löschen möchten.
3. Klicken Sie auf "Senden".

Migrieren der Aufgabenpersistenz-Datenbank

In früheren Versionen wurde Migrationen ungeplant und mithilfe der Management-Konsole durchgeführt. Ein Befehlszeilentool für die Migration wurde bereitgestellt, um bei der Migration großer Aufgabenmengen Leistungsengpässe zu verhindern. Sie können die Migration auch für eine bestimmte Umgebung, einen bestimmten Aufgabenstatus und für Aufgaben, die während eines bestimmten Datumsbereichs erstellt und ausgeführt wurden, optimieren. Das Befehlszeilentool "runmigration" befindet sich im folgenden Ordner:

```
admin_tools/tools/tpmigration
```

Gehen Sie folgendermaßen vor, um die Aufgabenpersistenz-Datenbank zu migrieren:

1. Aktualisieren Sie die Datei "tpmigration125.properties".
2. Legen Sie die JAVA_HOME-Variable fest.
3. Führen Sie das runmigration-Tool aus.

Aktualisieren der Datei "tpmigration125.properties"

Um die Migration der Aufgabenpersistenz-Datenbank einzurichten, müssen Sie die Datei "tpmigration.properties" mit den Objektspeicher- und Aufgabenpersistenzinformationen, einschließlich der Speicherwerte, aktualisieren. Die Datei "tpmigration125.properties" befindet sich im folgenden Verzeichnis:

<IAM Suite-Ordner>/tools/tpmigration/com/ca/tp/migratetpto125

Geben Sie die folgenden Informationen in der Eigenschaftsdatei an, um die Migration einzurichten:

```
############################################################
# The object store is required to obtain the environment details.
############################################################
os.db.hostname=<Hostname>
os.db.dbname=<Datenbankname oder SID>
os.db.username=<DB-Benutzername>
os.db.password=<DB-Benutzerkennwort>
os.db.port=<DB-Portnummer>
os.db.dbType=<Typ der Datenbank.  Zum Beispiel für SQL Server sql2005 und für Oracle
'oracle'>

############################################################
# Task persistence data where the old and new tables are.
############################################################
tp.db.hostname=<Hostname>
tp.db.dbname=<Datenbankname oder SID>
tp.db.username=<DB-Benutzername>
tp.db.password=<DB-Benutzerkennwort>
tp.db.port=<DB-Portnummer>
tp.db.dbType=<Typ der Datenbank.  Zum Beispiel für SQL Server sql2005 und für Oracle
'oracle'>
```

Festlegen der JAVA_HOME-Variable

Die Umgebungsvariable JAVA_HOME muss festgelegt sein, damit das runmigration-Tool ordnungsgemäß ausgeführt wird.

Ausführen des runmigration-Tools

Gehen Sie folgendermaßen vor, um die Migration zu starten.

Über eine Befehlszeile

1. Führen Sie das runmigration-Tool aus.

   Für Windows:

   ```
   runmigration.bat
   ```

   Für UNIX:

   ```
   runmigration.sh
   ```

2. Geben Sie folgende Daten ein:

   - Den geschützten Umgebungs-Alias ("Alle" für alle Umgebungen).

     Hinweis: Wenn Sie nicht "Alle" angeben, kann nur eine Umgebung eingegeben werden.

   - Den Aufgabenstatus.
     Hinweis: Wenn Sie nicht "alle" angeben, kann nur eine Aufgabe eingegeben werden.

   - Die CA IdentityMinder-Version, von der die Migration durchgeführt werden soll (1-8.x, 2-12.0).

   - Möchten Sie einen Datumsbereich für die zu migrierenden Aufgaben angeben (j/n)?

     Hinweis: Wenn Sie "j" wählen, müssen Sie Folgendes eingeben:

     - Startdatum (mm/dd/jj)
     - Enddatum (mm/dd/jj)

   Die Migration wird gestartet.

Nach dem Abschluss der Migration gibt der Status an, wie viele Aufgaben migriert wurden.